
To Trust Or Not To Trust A Classifier

Heinrich Jiang*

Google Research

heinrichj@google.com

Been Kim*

Google Brain

beenkim@google.com

Maya Gupta

Google Research

mayagupta@google.com

Abstract

Knowing when a classifier’s prediction can be trusted is useful in many applications and critical for safely using AI. While the bulk of the effort in machine learning research has been towards improving classifier performance, understanding when a classifier’s predictions should and should not be trusted has received far less attention. The standard approach is to use the classifier’s discriminant or confidence score; however, we show there exists a considerably more effective alternative.

We propose a new score, called the *trust score*, which measures the agreement between the classifier and a modified nearest-neighbor classifier on the testing example. We show empirically that high (low) trust scores produce surprisingly high precision at identifying correctly (incorrectly) classified examples, consistently outperforming the classifier’s confidence score as well as many other baselines.

Further, under some mild distributional assumptions, we show that if the trust score for an example is high (low), the classifier will likely agree (disagree) with the Bayes-optimal classifier. Our guarantees consist of non-asymptotic rates of statistical consistency under various nonparametric settings and build on recent developments in topological data analysis.

1 Introduction

Machine learning (ML) is a powerful and widely-used tool for making potentially important decisions, from product recommendations to medical diagnosis. However, despite ML’s impressive performance, it makes mistakes, with some more costly than others. While improving overall accuracy is an important goal that the bulk of the effort in ML community has been focused on, it may not be enough: we need to also better understand the strengths and limitations of ML techniques.

This work focuses on one such challenge: knowing whether a classifier’s prediction for a test example can be trusted or not. Such trust scores have tremendous practical applications. They can be directly shown to users to help them gauge whether they should trust the AI system. This is crucial when a model’s prediction influences important decisions such as a medical diagnosis, but can also be helpful even in low-stakes scenarios such as movie recommendations. Trust scores can be used to override the classifier and send the decision to a human operator, or to prioritize decisions that human operators should be making. Trust scores are also useful for monitoring classifiers to detect distribution shifts that may mean the classifier is no longer as useful as it was when launched.

A standard approach to deciding whether to trust a classifier’s decision is to use the classifiers’ own reported confidence or score, e.g. probabilities from the softmax layer of a neural network, distance to the separating hyperplane in support vector classification, mean class probabilities for the trees in

*Equal Contribution.

a random forest. While using a model’s own implied confidences appears reasonable, it has been shown that the raw confidence values from a classifier are poorly calibrated [23, 30]. Worse yet, even if the scores are calibrated, the ranking of the scores itself may not be reliable. In other words, a higher confidence score from the model does not necessarily imply higher probability that the classifier is correct, as shown in [39, 21, 34]. A classifier may simply not be the best judge of its own trustworthiness.

In this paper, we use a set of labeled examples as side information to help determine a classifier’s trustworthiness for a particular testing example. First, we propose a simple procedure that reduces the training data to a high density set for each class. Then we define the *trust score*—the ratio between the distance from the testing sample to the nearest class different from the predicted class and the distance to the predicted class—to determine whether to trust that classifier prediction. This simple test comes with comprehensive theoretical guarantees as well as strong empirical results. Theoretically, we show that high/low trust scores correspond to high probability of agreement/disagreement with the Bayes-optimal classifier. We show finite-sample estimation rates when the data is full-dimension and supported on or near a low-dimensional manifold. Interestingly, we attain bounds that depend only on the lower manifold dimension and independent of the ambient dimension without any changes to the procedure or knowledge of the manifold. To our knowledge, these results are new and may be of independent interest.

We empirically validate this idea on various set of classifiers, including logistic regression, random forest and deep neural networks such as InceptionV3 [45, 10]. We show that the precision of the trust score outperforms a set of baselines across benchmark datasets, both categorical and images data.

2 Related Work

One related line of work is that of confidence calibration, which transforms classifier outputs into values that can be interpreted as probabilities, e.g. [38, 52, 35, 23]. [30] which explore the structured prediction setting, and [31] obtain confidence estimates by using ensembles of networks. These calibration techniques typically only use the the model’s reported score (and the softmax layer in the case of a neural network) for calibration, which preserves the rankings of the classifier scores. Similarly, [25] considered using the softmax probabilities for the related problem of identifying misclassifications and mislabeled points.

Recent work explored estimating uncertainty for Bayesian neural networks [19, 29], returning a distribution over the outputs, by making a connection with dropout [44]. Our trust score does not change the network structure (nor does it assume any structure) and gives a single score, rather than a distribution over outputs as the representation of uncertainty.

The problem of classification with a reject option or learning with abstention [2, 51, 7, 22, 6, 26, 8] is a highly related framework where the classifier is allowed to abstain from making a prediction at a certain cost. Typically such methods jointly learn the classifier and the rejection function. Our paper assumes an already trained and possibly black-box classifier and learns the confidence scores separately, but we do not explicitly learn the appropriate rejection thresholds. The interplay between classification rate and reject rate is however studied in many various forms e.g. [5, 12, 18, 42, 47, 17, 32, 13, 50, 46].

Whether to trust a classifier also arises in the setting where one has access to a sequence of classifiers, but there is some cost to evaluating each classifier, and the goal is to decide after evaluating each classifier in the sequence if one should trust the current classifier decision enough to stop, rather than evaluating more classifiers in the sequence (e.g. [49, 37, 15]). Those confidence decisions are usually based on whether the current classifier score will match the classification of the full sequence.

Our work builds on recent results in topological data analysis. Our method to filter low-density points estimates a particular density level-set given a parameter α , which aims at finding the level-set that contains $1 - \alpha$ fraction of the probability mass. Level-set estimation has a long history [24, 14, 48, 43, 40, 27]. However such works assume knowledge of the density level, which is difficult to determine in practice. We provide rates for Algorithm 1 in estimating the appropriate level-set corresponding to α without knowledge of the level. To our knowledge this is the first time the proxy α , which is a more intuitive parameter compared to the density value, is used for level-set

estimation. Our analysis is also done under various settings including when the data lies near a lower dimensional manifold and we provide rates that depend only on the lower dimension.

3 Algorithm: The Trust Score

Our approach proceeds in two steps outlined in Algorithm 1 and 2. We first pre-process the training data, as described in Algorithm 1, to find the α -high-density-set of each class, which is defined as the training samples within that class after filtering out α -fraction of the samples with lowest density (which may be outliers):

Definition 1 (α -high-density-set). *Let f be a density function with compact support $\mathcal{X} \subseteq \mathbb{R}^D$ and $0 \leq \alpha < 1$. Then define $H_\alpha(f)$, the α -high-density-set of f , to be the λ_α -level set of f , defined as $\{x \in \mathcal{X} : f(x) \geq \lambda_\alpha\}$ where $\lambda_\alpha := \inf \{\lambda \geq 0 : \int_{\mathcal{X}} 1[f(x) \leq \lambda] f(x) dx \geq \alpha\}$.*

In order to approximate the α -high-density-set, Algorithm 1 filters the α -fraction of the sample points with lowest empirical density, based on k -nearest neighbors. This data filtering step is independent of the given classifier h . Then, the second step: given a testing sample, we define its *trust score* to be the ratio between the distance from the testing sample to the α -high-density-set of the nearest class different from the predicted class, and the distance from the test sample to the α -high-density-set of the class predicted by h , as detailed in Algorithm 2. The intuition is that if the classifier h predicts a label that is considerably farther than the closest label, then this is a warning that the classifier may be making a mistake.

Our procedure can thus be viewed as a comparison to a modified nearest-neighbor classifier, where the modification lies in the initial filtering of points not in the α -high-density-set for each class. We show in Section 4 that the proposed trust score can reveal signals from the Bayes-optimal classifier.

Algorithm 1 Estimating α -high-density-set

Parameters: α (density threshold), k .

Inputs: Sample points $X := \{x_1, \dots, x_n\}$ drawn from f .

Define k -NN radius $r_k(x) := \inf\{r > 0 : |B(x, r) \cap X| \geq k\}$ and let $\varepsilon := \inf\{r > 0 : |\{x \in X : r_k(x) > r\}| \leq \alpha \cdot n\}$.

return $\widehat{H}_\alpha(f) := \{x \in X : r_k(x) \leq \varepsilon\}$.

Algorithm 2 Trust Score

Parameters: α (density threshold), k .

Input: Classifier $h : \mathcal{X} \rightarrow \mathcal{Y}$. Training data $(x_1, y_1), \dots, (x_n, y_n)$. Test example x .

For each $\ell \in \mathcal{Y}$, let $\widehat{H}_\alpha(f_\ell)$ be the output of Algorithm 1 with parameters α, k and sample points $\{x_j : 1 \leq j \leq n, y_j = \ell\}$. Then, return the trust score, defined as:

$$\xi(h, x) := d\left(x, \widehat{H}_\alpha(f_{\tilde{h}(x)})\right) / d\left(x, \widehat{H}_\alpha(f_{h(x)})\right),$$

where $\tilde{h}(x) = \operatorname{argmin}_{l \in \mathcal{Y}, l \neq h(x)} d\left(x, \widehat{H}_\alpha(f_l)\right)$.

The trust score can be used as either a black-box method without using any of inner workings of classifier, or a white-box method where the distances are computed in some intermediate representational space of the classifier, such as a middle layer of a DNN. We show empirical results for both in Section 5.

The method has two hyperparameters: k (the number of neighbors, such as in k -NN) and α (fraction of data to filter) to compute the empirical densities. We show in theory that k can lie in a wide range and still give us the desired consistency guarantees. Throughout our experiments, we fix $k = 10$, and use cross-validation to select α as it is data-dependent.

4 Theoretical Analysis

In this section, we provide theoretical guarantees for Algorithms 1 and 2. Due to space constraints, all the proofs are deferred to the appendix. To simplify the main text, we state our results treating δ , the confidence level, as a constant. The dependence on δ in the rates is made explicit in the Appendix.

We show that Algorithm 1 is a statistically consistent estimator of the α -high-density-level set with finite-sample estimation rates. We analyze Algorithm 1 in three different settings. When the data lies on (i) full-dimensional \mathbb{R}^D ; (ii) an unknown lower dimensional submanifold embedded in \mathbb{R}^D ; and (iii) an unknown lower dimensional submanifold with full-dimensional noise.

For setting (i), where the data lies in \mathbb{R}^D , the estimation rate has a dependence on the dimension D , which may be unattractive in high-dimensional situations: this is known as the curse of dimensionality, suffered by density-based procedures in general. However, when the data has low intrinsic dimension in (ii), it turns out that, remarkably, without any changes to the procedure, the estimation rate depends on the lower dimension d and is *independent* of the ambient dimension D . However, in realistic situations, the data may not lie *exactly* on a lower-dimensional manifold, but *near* one. This reflects the setting of (iii), where the data essentially lies on a manifold but has general full-dimensional noise so the data is overall full-dimensional. Interestingly, we show that we still obtain estimation rates depending only on the manifold dimension and independent of the ambient dimension; moreover, we don't require knowledge of the manifold nor its dimension to attain these rates.

We then analyze Algorithm 2, and establish the culminating result of Theorem 4: for labeled data distributions with well-behaved class margins, when the trust score is large, the classifier likely agrees with the Bayes-optimal classifier, and when the trust score is small, the classifier likely disagrees with the Bayes-optimal classifier. If it turns out that even the Bayes-optimal classifier has high-error in a certain region, then any classifier will have difficulties in that region. Thus, this result does not guarantee that the trust score can predict misclassification, but rather that the classifier has a relatively high chance of not making the right decision, where high chance might mean close to fifty percent for a binary classifier.

4.1 Analysis of Algorithm 1

We require the following regularity assumptions on the boundaries of $H_\alpha(f)$, which are standard in analyses of level-set estimation [43]. Assumption 1.1 ensures that the density around $H_\alpha(f)$ has both smoothness and curvature. The upper bound gives smoothness, which is important to ensure that our density estimators are accurate for our analysis (we only require this smoothness near the boundaries and not globally). The lower bound ensures curvature: this ensures that $H_\alpha(f)$ is salient enough to be estimated. Assumption 1.2 ensures that $H_\alpha(f)$ doesn't get arbitrarily thin anywhere.

Assumption 1 (α -high-density-set regularity). *Let $\beta > 0$. There exists $\check{C}_\beta, \hat{C}_\beta, \beta, r_c, r_0, \rho > 0$ s.t.*

1. $\check{C}_\beta \cdot d(x, H_\alpha(f))^\beta \leq |\lambda_\alpha - f(x)| \leq \hat{C}_\beta \cdot d(x, H_\alpha(f))^\beta$ for all $x \in \partial H_\alpha(f) + B(0, r_c)$.
2. For all $0 < r < r_0$ and $x \in H_\alpha(f)$, we have $\text{Vol}(B(x, r)) \geq \rho \cdot r^D$.

where ∂A denotes the boundary of a set A , $d(x, A) := \inf_{x' \in A} \|x - x'\|$, $B(x, r) := \{x' : |x - x'| \leq r\}$ and $A + B(0, r) := \{x : d(x, A) \leq r\}$.

Our statistical guarantees are under the Hausdorff metric, which ensures a *uniform* guarantee over our estimator: it is a stronger notion of consistency than other common metrics [40, 41].

Definition 2 (Hausdorff distance). $d_H(A, B) := \max\{\sup_{x \in A} d(x, B), \sup_{x \in B} d(x, A)\}$.

We now give the following result for Algorithm 1. It says that as long as our density function satisfies the regularity assumptions stated earlier, and the parameter k lies within a certain range, then we can bound the Hausdorff distance between what Algorithm 1 recovers and $H_\alpha(f)$, the true α -high-density set, from an i.i.d. sample drawn from f of size n . Then, as n goes to ∞ , and k grows as a function of n , the quantity goes to 0.

Theorem 1 (Algorithm 1 guarantees). *Let $0 < \delta < 1$ and suppose that f is continuous and has compact support $\mathcal{X} \subseteq \mathbb{R}^D$ and satisfies Assumption 1. There exists constants $C_l, C_u, C > 0$ depending on f and δ such that the following holds with probability at least $1 - \delta$. Suppose that k satisfies $C_l \cdot \log n \leq k \leq C_u \cdot (\log n)^{D(2\beta+D)} \cdot n^{2\beta/(2\beta+D)}$. Then we have*

$$d_H(H_\alpha(f), \widehat{H}_\alpha(f)) \leq C \cdot \left(n^{-1/2D} + \log(n)^{1/2\beta} \cdot k^{-1/2\beta} \right).$$

Remark 1. The condition on k can be simplified by ignoring log factors: $\log n \lesssim k \lesssim n^{2\beta/(2\beta+D)}$, which is a wide range. When optimizing k , we obtain our consistency guarantee of

$$d_H(H_\alpha(f), \widehat{H}_\alpha(f)) \lesssim \max\{n^{-1/2D}, n^{-1/(2\beta+D)}\}.$$

The first term is due to the error from estimating the appropriate level given α (i.e. identifying the level λ_α) and the second term corresponds to the error for recovering the level set given knowledge of the level. The latter term matches the lower bound for level-set estimation up to log factors [48].

4.2 Analysis of Algorithm 1 on Manifolds

One of the disadvantages of the last result is that the estimations errors have a dependence on D , the dimension of the data, which may be highly undesirable in high-dimensional settings seen in practice. We next improve these rates when the data has a lower intrinsic dimension. Interestingly, we are able to show rates that depend only on the intrinsic dimension of the data, without explicit knowledge of that dimension nor any changes to the procedure. As common to related work in the manifold setting, we make the following regularity assumptions which are standard among works in manifold learning e.g. [36, 20, 1].

Assumption 2 (Manifold Regularity). *M is a d -dimensional smooth compact Riemannian manifold without boundary embedded in compact subset $\mathcal{X} \subseteq \mathbb{R}^D$ with bounded volume. M has finite condition number $1/\tau$, which controls the curvature and prevents self-intersection.*

Theorem 2 (Manifold analogue of Theorem 1). *Let $0 < \delta < 1$. Suppose that density function f is continuous and supported on M and Assumptions 1 and 2 hold. Suppose also that there exists $\lambda_0 > 0$ such that $f(x) \geq \lambda_0$ for all $x \in M$. Then, there exists constants $C_l, C_u, C > 0$ depending on f and δ such that the following holds with probability at least $1 - \delta$. Suppose that k satisfies $C_l \cdot \log n \leq k \leq C_u \cdot (\log n)^{d(2\beta' + d)} \cdot n^{2\beta'/(2\beta' + d)}$, where $\beta' := \max\{1, \beta\}$. Then we have*

$$d_H(H_\alpha(f), \widehat{H}_\alpha(f)) \leq C \cdot \left(n^{-1/2d} + \log(n)^{1/2\beta} \cdot k^{-1/2\beta} \right).$$

Remark 2. When optimizing k , we obtain (ignoring log factors)

$$d_H(H_\alpha(f), \widehat{H}_\alpha(f)) \lesssim \max\{n^{-1/2d}, n^{-1/(2 \max\{1, \beta\} + d)}\}.$$

The first term can be compared to that of the previous result where D is replaced with d . The second term is the error for recovering the level set on manifolds, which matches recent rates [27].

4.3 Analysis of Algorithm 1 on Manifolds with Full Dimensional Noise

In realistic settings, the data may not lie exactly on a low-dimensional manifold, but *near* one. We next present a result where the data is distributed along a manifold with additional full-dimensional noise. We make little assumptions on the noise distribution. Thus, in this situation, the data has intrinsic dimension equal to the ambient dimension. Interestingly, we are still able to show that the rates only depend on the dimension of the manifold and not the dimension of the entire data.

Theorem 3. *Let $0 < \eta < \alpha < 1$ and $0 < \delta < 1$. Suppose that distribution \mathcal{F} is a weighted mixture $(1 - \eta) \cdot \mathcal{F}_M + \eta \cdot \mathcal{F}_E$ where \mathcal{F}_M is a distribution with continuous density f_M supported on a d -dimensional manifold M satisfying Assumption 2 and \mathcal{F}_E is a (noise) distribution with continuous density f_E with compact support over \mathbb{R}^D with $d < D$. Suppose also that there exists $\lambda_0 > 0$ such that $f_M(x) \geq \lambda_0$ for all $x \in M$ and $H_{\tilde{\alpha}}(f_M)$ (where $\tilde{\alpha} := \frac{\alpha - \eta}{1 - \eta}$) satisfies Assumption 1 for density f_M . Let \widehat{H}_α be the output of Algorithm 1 on a sample X of size n drawn i.i.d. from \mathcal{F} . Then, there exists constants $C_l, C_u, C > 0$ depending on f_M, f_E, η, M and δ such that the following holds with probability at least $1 - \delta$. Suppose that k satisfies $C_l \cdot \log n \leq k \leq C_u \cdot (\log n)^{d(2\beta' + d)} \cdot n^{2\beta'/(2\beta' + d)}$, where $\beta' := \max\{1, \beta\}$. Then we have*

$$d_H(H_{\tilde{\alpha}}(f_M), \widehat{H}_\alpha) \leq C \cdot \left(n^{-1/2d} + \log(n)^{1/2\beta} \cdot k^{-1/2\beta} \right).$$

The above result is attractive because it begins to show why our methods can work, even in high-dimensions, despite the curse of dimensionality of non-parametric methods. In typical real-world data, even if the data lies in a high-dimensional space, there may be far fewer degrees of freedom. Thus, our theoretical results suggest that if this is true, then our methods will enjoy far better convergence rates – even when the data overall has full intrinsic dimension due to factors such as noise.

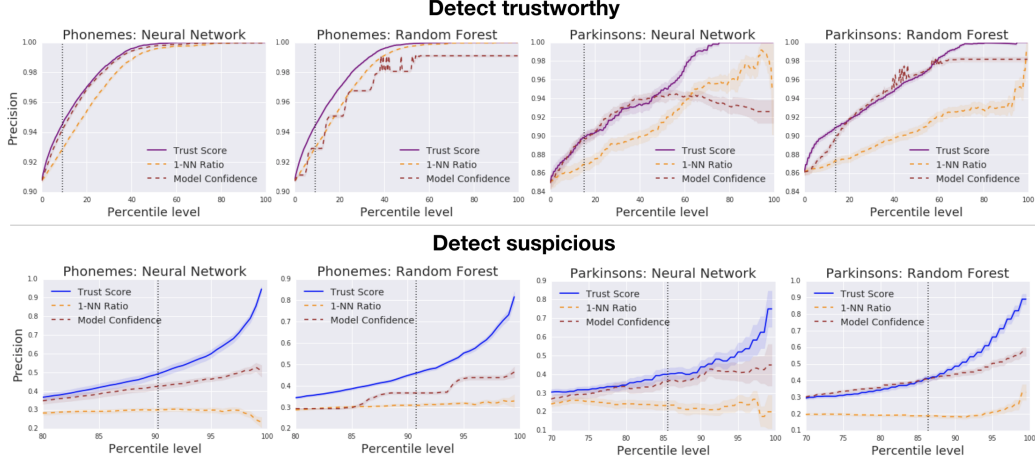


Figure 1: Two example datasets and models. Predicting correctness (top row) and incorrectness (bottom) (see appendix for the model baselines and full results). The vertical dotted black line indicates accuracy level of the classifier. The trust score consistently attains a higher precision for each given percentile of classifier decision-rejection. Furthermore, the trust score generally shows increasing precision as the percentile level increases, but surprisingly, many of the comparison baselines do not.

4.4 Analysis of Algorithm 2: the Trust Score

We now provide a guarantee about the trust score, making the same assumptions as in Theorem 3 for each of the label distributions. We additionally assume that the class distributions are well-behaved in the following sense: that high-density-regions for each of the classes satisfy the property that for any point $x \in \mathcal{X}$, if the ratio of the distance to one class's high-density-region to that of another is smaller by some margin γ , then it is more likely that x 's label corresponds to the former class.

Theorem 4. *Let $0 < \eta < \alpha < 1$. Let us have labeled data $(x_1, y_1), \dots, (x_n, y_n)$ drawn from distribution \mathcal{D} , which is a joint distribution over $\mathcal{X} \times \mathcal{Y}$ where \mathcal{Y} are the labels, $|\mathcal{Y}| < \infty$, and $\mathcal{X} \subseteq \mathbb{R}^D$ is compact. Suppose for each $\ell \in \mathcal{Y}$, the conditional distribution for label ℓ which satisfies the conditions of Theorem 3 for some manifold M and noise level η . Let $f_{M,\ell}$ be the density of the portion of the conditional distribution supported on M . Define $M_\ell := H_{\tilde{\alpha}}(f_\ell)$, where $\tilde{\alpha} := \frac{\alpha - \eta}{1 - \eta}$ and let ϵ_n be the maximum Hausdorff error from estimating M_ℓ over each $\ell \in \mathcal{Y}$ in Theorem 3. Assume that $\min_{\ell \in \mathcal{Y}} \mathbb{P}_{\mathcal{D}}(y = \ell) > 0$ to ensure we have sufficient samples from each label.*

Suppose also that for each $x \in \mathcal{X}$, if $d(x, M_i)/d(x, M_j) < 1 - \gamma$ then $\mathbb{P}(y = i|x) > \mathbb{P}(y = j|x)$ for $i, j \in \mathcal{Y}$. That is, if we are closer to M_i than M_j by a ratio of less than $1 - \gamma$, then the point is more likely to be from class i . Let h^ be the Bayes-optimal classifier, defined by $h^*(x) := \operatorname{argmax}_{\ell \in \mathcal{Y}} \mathbb{P}(y = \ell|x)$. Then, the trust score ξ of Algorithm 2, satisfies the following with high probability uniformly in $x \in \mathcal{X}$ and classifiers $h : \mathcal{X} \rightarrow \mathcal{Y}$ for n sufficiently large depending on \mathcal{D} .*

$$\begin{aligned} \xi(h, x) < 1 - \gamma - \frac{\epsilon_n}{d(x, M_{h(x)}) + \epsilon_n} \cdot \left(\frac{d(x, M_{\tilde{h}(x)})}{d(x, M_{h(x)})} + 1 \right) &\Rightarrow h(x) \neq h^*(x), \\ \frac{1}{\xi(h, x)} < 1 - \gamma - \frac{\epsilon_n}{d(x, M_{\tilde{h}(x)}) + \epsilon_n} \cdot \left(\frac{d(x, M_{h(x)})}{d(x, M_{\tilde{h}(x)})} + 1 \right) &\Rightarrow h(x) = h^*(x). \end{aligned}$$

5 Experiments

In this section, we show empirically that trust scores can both detect examples that are incorrectly classified with high precision and be used as a signal to determine which examples are likely correct. We perform this evaluation across (i) different datasets (Section 5.1) (ii) different families of classifiers (neural network, random forest and logistic regression) (Section 5.1) (iii) different tunings of the

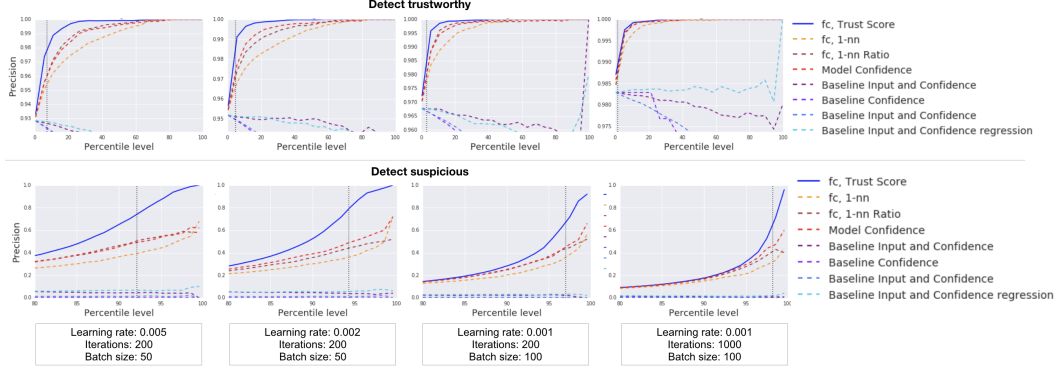


Figure 2: MNIST: Three different models (each column) as well as precision on identifying correctly classified (top) and incorrectly classified (bottom) examples. The baselines’ curves have a widening gap compared to our methods when model achieves lower accuracy. The accuracy level of the neural network (indicated by the vertical dotted black lines) increase from left to right. "fc" is a fully-connected layer in the network. See Appendix for the full figure.

classifier (Section 5.2) and (iv) different representations of the data e.g. input data or activations of various intermediate layers in a neural network (Section 5.3).

To evaluate the effectiveness of trust scores and baselines we use the following process. Each method produces a numeric score for each testing example. For each method, we bin the data points by percentile value of the score (i.e. 100 bins). Then, given a recall percentile level (i.e. the x -axis on our plots), we take the performance of the classifier on the bins above the percentile level as the precision (i.e. the y -axis). For identifying suspicious examples, the precision is the misclassification rate and for identifying trustworthy examples, we take the negative of each method’s score and use the accuracy of the classifier. In any case, the higher the precision vs percentile curve, the better the method.

Baselines used: The first baseline we use is the model’s own confidence score, which is similar to the approach of [25]. While calibrating the classifiers’ confidence scores (i.e. transforming them into probability estimates of correctness) is an important related work [23, 38], such techniques typically do not change the rankings of the score, at least in the binary case. Since we evaluate the trust score on its precision at a given recall *percentile level*, we are interested in the relative *ranking* of the scores rather than their absolute values. Thus, we do not compare against calibration techniques. There are surprisingly few methods aimed at identifying correctly or incorrectly classified examples with precision at a recall percentile level as noted in [25].

We give two additional types of baselines: *distance* baselines and *model* baselines. The distance baselines use the distances between the testing example and α -high-density-sets for each class. We use two distance baselines: (i) the *nearest neighbor ratio* (1-nn ratio), which is the distance ratio between the closest and second closest α -high-density-set, which can be viewed as an analogue to the trust score without knowledge of the classifier; and (ii) the *nearest neighbor softmax* (1-nn), which is the distance between testing example and the closest α -high-density-set, normalized by the sum of distances to all other classes. The model baselines involve training a separate neural network to predict whether the classifier will misclassify the example. We have four such model baselines: three of them are neural network classifiers that takes some combination of the feature vectors and the classifier’s confidence, and output a prediction of whether the classifier is misclassifying. The last model baseline is a regression NN model that takes feature vectors and the classifier’s confidence to predict if the classifier is misclassifying.

Choosing Hyperparameters: The two hyperparameters for the trust score are α and k . Throughout the experiments, we fix $k = 10$ and choose α using cross-validation over (negative) powers of 2. The bulk of the computational cost for the trust-score is in k -nearest neighbor computations for training and 1-nearest neighbor searches for evaluation. To speed things up for the high-dimensional datasets MNIST and ImageNet, we reduced the data down to 20 dimensions using PCA before being processed by the trust score. Interestingly, even with this reduction, the trust score maintains high

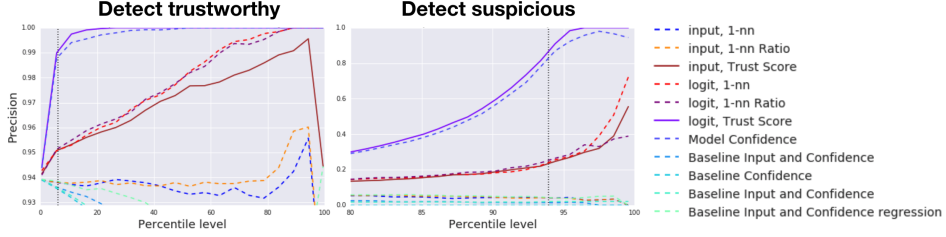


Figure 3: InceptionV3: precision on correct (left) and incorrect (right) precision. In general, our method returns higher performance with deeper layers (closer to logit) than with lower layers. See Appendix for the full figure.

performance. We note that any approximation method (such as approximate instead of exact nearest neighbors) could have been used instead.

5.1 Performance Across Various Datasets and Models

In this section, we show performance on five benchmark UCI datasets [16] and the Phonemes dataset of [11], each for three kinds of classifiers (neural network, random forest and logistic regression). Due to space, we only show two data sets and two models in Figure 1. The rest can be found in the Appendix. For each method and dataset, we evaluated with multiple runs. For each run we took a random stratified split of the dataset into two halves. One half was used for training the trust score and the other half was used for evaluation and the standard error is shown in addition to the average precision across the runs at each percentile level. The results show that our method consistently has a higher precision vs percentile curve than the rest of the methods across the datasets and models. This suggests the trust score considerably improves upon known methods as a signal for identifying trustworthy and suspicious testing examples.

5.2 Performance Over Different Model Training Hyperparameters

In this section, we train a neural network on the MNIST dataset [33] for a fixed model architecture, and vary the batch size and learning rate. As a consequence, the performance of the classifier will also vary. Four models with varying accuracy (vertical dotted black line) are shown in Figure 2. The results show that as the classifier’s accuracy increases, it becomes harder to detect suspicious examples. However, it was not easier to detect which examples are trustworthy for the more accurate classifiers. Throughout, the trust score consistently outperforms the baselines (only a few examples are shown in Figure 2; a full analysis is in the Appendix).

5.3 Evaluating the Trust Score on Neural Network Intermediate Layers

One simple generalization of our method is to use intermediate layers of a neural network as an input instead of the raw x . Prior work (e.g., [53]) suggests that a neural network seems to learn useful but different representations of x at each layer. For this experiment, we use the ImageNet dataset with Inceptionv3 model, which contains 10 intermediate layers, thus offering a variety of representations. Figure 4 shows that in general, our method has better performance with deeper layers (closer to logit) than with lower layers. This observation may be explained by many prior work which showed that lower layers learn lower level features, such as edges in the image, which then are combined to conduct higher level reasoning in deeper layers. It is plausible that higher level reasoning is better and necessary for predicting trustworthiness. We include baseline results for InceptionV3 in Figure 3 and the experiment details in Appendix. Note that baseline models are out of range in the figure. See the Appendix for the full chart.

Conclusion:

In this paper, we provide the *trust score*: a new, simple, and effective way to judge if one should trust the prediction from a classifier. We show high-probability non-asymptotic statistical guarantees that high (low) trust scores correspond to agreement (disagreement) with the Bayes-optimal classifier

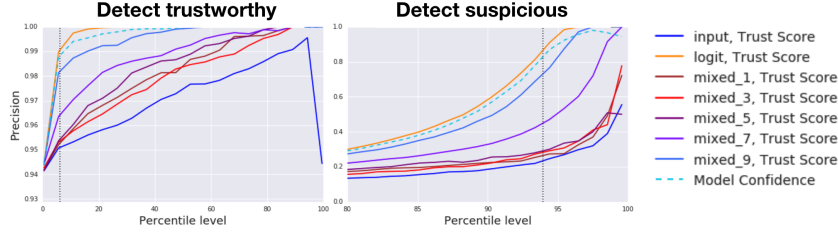


Figure 4: InceptionV3: precision on correct (left) and incorrect (right) precision. Higher layers generally seems to achieve better precision.

under various nonparametric settings, which build on recent results in topological data analysis. Our empirical results across many datasets, classifiers, and representations of the data show that our method consistently outperforms the classifier’s own reported confidence as well as many baselines in identifying trustworthy and suspicious examples. The theoretical and empirical results suggest that this approach may have significant practical implications.

References

- [1] Sivaraman Balakrishnan, Srivatsan Narayanan, Alessandro Rinaldo, Aarti Singh, and Larry Wasserman. Cluster trees on manifolds. In *Advances in Neural Information Processing Systems*, pages 2679–2687, 2013.
- [2] Peter L Bartlett and Marten H Wegkamp. Classification with a reject option using a hinge loss. *Journal of Machine Learning Research*, 9(Aug):1823–1840, 2008.
- [3] Kamalika Chaudhuri and Sanjoy Dasgupta. Rates of convergence for the cluster tree. In *Advances in Neural Information Processing Systems*, pages 343–351, 2010.
- [4] Frédéric Chazal. An upper bound for the volume of geodesic balls in submanifolds of euclidean spaces. *Personal Communication*, available at <http://geometrica.saclay.inria.fr/team/Fred.Chazal/BallVolumeJan2013.pdf>, 2013.
- [5] C Chow. On optimum recognition error and reject tradeoff. *IEEE Transactions on information theory*, 16(1):41–46, 1970.
- [6] Corinna Cortes, Giulia DeSalvo, and Mehryar Mohri. Boosting with abstention. In *Advances in Neural Information Processing Systems*, pages 1660–1668, 2016.
- [7] Corinna Cortes, Giulia DeSalvo, and Mehryar Mohri. Learning with rejection. In *International Conference on Algorithmic Learning Theory*, pages 67–82. Springer, 2016.
- [8] Corinna Cortes, Giulia DeSalvo, Claudio Gentile, Mehryar Mohri, and Scott Yang. Online learning with abstention. *arXiv preprint arXiv:1703.03478*, 2017.
- [9] Sanjoy Dasgupta and Samory Kpotufe. Optimal rates for k-NN density and mode estimation. In *Advances in Neural Information Processing Systems*, pages 2555–2563, 2014.
- [10] J. Deng, W. Dong, R. Socher, L.J. Li, K. Li, and L. Fei-Fei. Imagenet: A large-scale hierarchical image database. In *CVPR*, 2009.
- [11] Dua Dheeru and Efi Karra Taniskidou. UCI machine learning repository. 2017. URL <http://archive.ics.uci.edu/ml>.
- [12] Bernard Dubuisson and Mylene Masson. A statistical decision rule with incomplete knowledge about classes. *Pattern recognition*, 26(1):155–165, 1993.
- [13] Ran El-Yaniv and Yair Wiener. On the foundations of noise-free selective classification. *Journal of Machine Learning Research*, 11(May):1605–1641, 2010.

- [14] Martin Ester, Hans-Peter Kriegel, Jörg Sander, Xiaowei Xu, et al. A density-based algorithm for discovering clusters in large spatial databases with noise. In *Kdd*, pages 226–231, 1996.
- [15] Wei Fan, Fang Chu, Haixun Wang, and Philip S. Yu. Pruning and dynamic scheduling of cost-sensitive ensembles. *AAAI*, 2002.
- [16] Jerome Friedman, Trevor Hastie, and Robert Tibshirani. The elements of statistical learning. 1, 2001.
- [17] Giorgio Fumera and Fabio Roli. Support vector machines with embedded reject option. In *Pattern recognition with support vector machines*, pages 68–82. Springer, 2002.
- [18] Giorgio Fumera, Fabio Roli, and Giorgio Giacinto. Multiple reject thresholds for improving classification reliability. In *Joint IAPR International Workshops on Statistical Techniques in Pattern Recognition (SPR) and Structural and Syntactic Pattern Recognition (SSPR)*, pages 863–871. Springer, 2000.
- [19] Yarin Gal and Zoubin Ghahramani. Dropout as a Bayesian approximation: Representing model uncertainty in deep learning. In *International Conference on Machine Learning*, pages 1050–1059, 2016.
- [20] Christopher Genovese, Marco Perone-Pacifico, Isabella Verdinelli, and Larry Wasserman. Minimax manifold estimation. *Journal of machine learning research*, 13(May):1263–1291, 2012.
- [21] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*, 2014.
- [22] Yves Grandvalet, Alain Rakotomamonjy, Joseph Keshet, and Stéphane Canu. Support vector machines with a reject option. In *Advances in neural information processing systems*, pages 537–544, 2009.
- [23] Chuan Guo, Geoff Pleiss, Yu Sun, and Kilian Q Weinberger. On calibration of modern neural networks. *arXiv preprint arXiv:1706.04599*, 2017.
- [24] John A Hartigan. Clustering algorithms. 1975.
- [25] Dan Hendrycks and Kevin Gimpel. A baseline for detecting misclassified and out-of-distribution examples in neural networks. *arXiv preprint arXiv:1610.02136*, 2016.
- [26] Radu Herbei and Marten H Wegkamp. Classification with reject option. *Canadian Journal of Statistics*, 34(4):709–721, 2006.
- [27] Heinrich Jiang. Density level set estimation on manifolds with DBSCAN. In *International Conference on Machine Learning*, pages 1684–1693, 2017.
- [28] Heinrich Jiang. Uniform convergence rates for kernel density estimation. In *International Conference on Machine Learning*, pages 1694–1703, 2017.
- [29] Alex Kendall and Yarin Gal. What uncertainties do we need in Bayesian deep learning for computer vision? In *Advances in Neural Information Processing Systems*, pages 5580–5590, 2017.
- [30] Volodymyr Kuleshov and Percy S Liang. Calibrated structured prediction. In *Advances in Neural Information Processing Systems*, pages 3474–3482, 2015.
- [31] Balaji Lakshminarayanan, Alexander Pritzel, and Charles Blundell. Simple and scalable predictive uncertainty estimation using deep ensembles. In *Advances in Neural Information Processing Systems*, pages 6405–6416, 2017.
- [32] Thomas CW Landgrebe, David MJ Tax, Pavel Paclík, and Robert PW Duin. The interaction between classification and reject performance for distance-based reject-option classifiers. *Pattern Recognition Letters*, 27(8):908–917, 2006.

- [33] Yann LeCun. The mnist database of handwritten digits. <http://yann.lecun.com/exdb/mnist/>, 1998.
- [34] Anh Nguyen, Jason Yosinski, and Jeff Clune. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 427–436, 2015.
- [35] Alexandru Niculescu-Mizil and Rich Caruana. Predicting good probabilities with supervised learning. In *Proceedings of the 22nd international conference on Machine learning*, pages 625–632. ACM, 2005.
- [36] Partha Niyogi, Stephen Smale, and Shmuel Weinberger. Finding the homology of submanifolds with high confidence from random samples. *Discrete & Computational Geometry*, 39(1-3): 419–441, 2008.
- [37] Nathan Parrish, Hyrum S. Anderson, Maya R. Gupta, and Dun Yu Hsaio. Classifying with confidence from incomplete information. *Journal of Machine Learning Research*, 14(December): 3561–3589, 2013.
- [38] John Platt et al. Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods. *Advances in large margin classifiers*, 10(3):61–74, 1999.
- [39] Foster J Provost, Tom Fawcett, and Ron Kohavi. The case against accuracy estimation for comparing induction algorithms. In *ICML*, volume 98, pages 445–453, 1998.
- [40] Philippe Rigollet, Régis Vert, et al. Optimal rates for plug-in estimators of density level sets. *Bernoulli*, 15(4):1154–1178, 2009.
- [41] Alessandro Rinaldo and Larry Wasserman. Generalized density clustering. *The Annals of Statistics*, 38(5):2678–2722, 2010.
- [42] Carla M Santos-Pereira and Ana M Pires. On optimal reject rules and roc curves. *Pattern recognition letters*, 26(7):943–952, 2005.
- [43] Aarti Singh, Clayton Scott, Robert Nowak, et al. Adaptive Hausdorff estimation of density level sets. *The Annals of Statistics*, 37(5B):2760–2782, 2009.
- [44] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Dropout: A simple way to prevent neural networks from overfitting. *The Journal of Machine Learning Research*, 15(1):1929–1958, 2014.
- [45] Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jon Shlens, and Zbigniew Wojna. Rethinking the inception architecture for computer vision. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 2818–2826, 2016.
- [46] David MJ Tax and Robert PW Duin. Growing a multi-class classifier with a reject option. *Pattern Recognition Letters*, 29(10):1565–1570, 2008.
- [47] Francesco Tortorella. An optimal reject rule for binary classifiers. In *Joint IAPR International Workshops on Statistical Techniques in Pattern Recognition (SPR) and Structural and Syntactic Pattern Recognition (SSPR)*, pages 611–620. Springer, 2000.
- [48] Alexandre B Tsybakov et al. On nonparametric estimation of density level sets. *The Annals of Statistics*, 25(3):948–969, 1997.
- [49] Joseph Wang, Kirill Trapeznikov, and Venkatesh Saligrama. Efficient learning by directed acyclic graph for resource constrained prediction. *Advances in Neural Information Processing Systems (NIPS)*, 2015.
- [50] Yair Wiener and Ran El-Yaniv. Agnostic selective classification. In *Advances in neural information processing systems*, pages 1665–1673, 2011.
- [51] Ming Yuan and Marten Wegkamp. Classification methods with reject option based on convex risk minimization. *Journal of Machine Learning Research*, 11(Jan):111–130, 2010.

- [52] Bianca Zadrozny and Charles Elkan. Transforming classifier scores into accurate multiclass probability estimates. In *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 694–699. ACM, 2002.
- [53] Matthew D Zeiler and Rob Fergus. Visualizing and understanding convolutional networks. In *European conference on computer vision*, pages 818–833. Springer, 2014.

Appendix

A Supporting results for Theorem 1 Proof

We need the following result giving guarantees on the empirical balls.

Lemma 1 (Uniform convergence of balls [3]). *Let \mathcal{F} be the distribution corresponding to f and \mathcal{F}_n be the empirical distribution corresponding to the sample X . Pick $0 < \delta < 1$. Assume that $k \geq D \log n$. Then with probability at least $1 - \delta$, for every ball $B \subset \mathbb{R}^D$ we have*

$$\begin{aligned}\mathcal{F}(B) &\geq C_{\delta,n} \frac{\sqrt{D \log n}}{n} \Rightarrow \mathcal{F}_n(B) > 0 \\ \mathcal{F}(B) &\geq \frac{k}{n} + C_{\delta,n} \frac{\sqrt{k}}{n} \Rightarrow \mathcal{F}_n(B) \geq \frac{k}{n} \\ \mathcal{F}(B) &\leq \frac{k}{n} - C_{\delta,n} \frac{\sqrt{k}}{n} \Rightarrow \mathcal{F}_n(B) < \frac{k}{n}.\end{aligned}$$

where $C_{\delta,n} = 16 \log(2/\delta) \sqrt{D \log n}$

Remark 3. *For the rest of the paper, many results are qualified to hold with probability at least $1 - \delta$. This often precisely the event in which Lemma 1 holds.*

Remark 4. *If $\delta = 1/n$, then $C_{\delta,n} = O((\log n)^{3/2})$.*

To analyze Algorithm 1, we need the following bounds on k -NN density estimation.

Definition 3. *Define the k -NN radius of $x \in \mathbb{R}^D$ as*

$$r_k(x) := \inf\{r > 0 : |X \cap B(x, r)| \geq k\},$$

Definition 4 (k -NN Density Estimator).

$$f_k(x) := \frac{k}{n \cdot v_D \cdot r_k(x)^D}.$$

where v_D is the volume of a unit ball in \mathbb{R}^D .

We can utilize such bounds from [9], which are repeated here.

Define the following one-sided modulus of continuity which characterizes how much the density increases locally:

$$\hat{r}(\epsilon, x) := \sup \left\{ r : \sup_{x' \in B(x, r)} f(x') - f(x) \leq \epsilon \right\}.$$

Lemma 2 (Lemma 3 of [9]). *Suppose that $k \geq 4C_{\delta,n}^2$. Then with probability at least $1 - \delta$, the following holds for all $x \in \mathbb{R}^D$ and $\epsilon > 0$.*

$$f_k(x) < \left(1 + 2 \frac{C_{\delta,n}}{\sqrt{k}}\right) (f(x) + \epsilon),$$

provided k satisfies $v_D \cdot \hat{r}(x, \epsilon)^D \cdot (f(x) + \epsilon) \geq \frac{k}{n} + C_{\delta,n} \frac{\sqrt{k}}{n}$.

Analogously, define the following which characterizes how much the density decreases locally.

$$\check{r}(\epsilon, x) := \sup \left\{ r : \sup_{x' \in B(x, r)} f(x) - f(x') \leq \epsilon \right\}.$$

Lemma 3 (Lemma 4 of [9]). *Suppose that $k \geq 4C_{\delta,n}^2$. Then with probability at least $1 - \delta$, the following holds for all $x \in \mathbb{R}^D$ and $\epsilon > 0$.*

$$f_k(x) \geq \left(1 - 2 \frac{C_{\delta,n}}{\sqrt{k}}\right) (f(x) - \epsilon),$$

provided k satisfies $v_D \cdot \check{r}(x, \epsilon)^D \cdot (f(x) - \epsilon) \geq \frac{k}{n} - C_{\delta,n} \frac{\sqrt{k}}{n}$.

B Proof of Theorem 1

It will be understood that in this section, we assume the conditions of Theorem 1. We first show that λ_α , that is the density level corresponding to the α -high-density-set is smooth in α .

Lemma 4. *There exists a constants $C_1, r_1 > 0$ depending on f such that the following holds for all $0 < \epsilon < r_1$ such that*

$$0 < \lambda_\alpha - \lambda_{\alpha-\epsilon} \leq C_1 \epsilon^{\beta/D} \text{ and } 0 < \lambda_{\alpha+\epsilon} - \lambda_\alpha \leq C_1 \epsilon^{\beta/D}$$

Proof. We have by definition that

$$\epsilon = \int_{\mathcal{X}} 1[\lambda_{\alpha-\epsilon} < f(x) \leq \lambda_\alpha] \cdot f(x) dx \geq \lambda_{\alpha-\epsilon} \int_{\mathcal{X}} 1[\lambda_{\alpha-\epsilon} < f(x) \leq \lambda_\alpha] dx.$$

Choosing ϵ sufficiently small such that Assumption 1 holds, we have

$$\begin{aligned} & \lambda_{\alpha-\epsilon} \int_{\mathcal{X}} 1[\lambda_{\alpha-\epsilon} < f(x) \leq \lambda_\alpha] dx \\ & \geq \lambda_{\alpha-\epsilon} \cdot \text{Vol} \left(\left(H_\alpha(x) + B \left(0, ((\lambda_{\alpha-\epsilon} - \lambda_\alpha)/\widehat{C}_\beta)^{1/\beta} \right) \right) \setminus H_\alpha(f) \right) \\ & \geq \lambda_{\alpha-\epsilon} \cdot C' ((\lambda_{\alpha-\epsilon} - \lambda_\alpha)/\widehat{C}_\beta)^{D/\beta} \end{aligned}$$

where the last inequality holds for some constant C' depending on f and Vol is the volume w.r.t. to the Lebesgue measure in \mathbb{R}^D . It then follows that

$$\lambda_{\alpha-\epsilon} - \lambda_\alpha \leq \widehat{C}_\beta \left(\frac{\epsilon}{\lambda_{\alpha-\epsilon} \cdot C'} \right)^{\beta/D}$$

and the result for the first part follows by taking $C_1 \leq \widehat{C}_\beta \cdot (\lambda_{\alpha-r_1} \cdot C')^{-\beta/D}$ and $r_1 < \alpha$. Showing that $0 < \lambda_{\alpha+\epsilon} - \lambda_\alpha \leq C_1 \epsilon^{\beta/D}$ can be done analogously and is omitted here. \square

The next result gets a handle on the density level corresponding to α returned by Algorithm 1.

Lemma 5. *Let $0 < \delta < 1$. Let $\widehat{\epsilon}$ be the ϵ setting chosen by Algorithm 1. Define*

$$\widehat{\lambda}_\alpha := \frac{k}{v_D \cdot n \cdot \widehat{\epsilon}^D}.$$

Then, with probability at least $1 - \delta$, we have there exist constant $C_1 > 0$ depending on f such that for n sufficiently large depending on f , we have

$$|\widehat{\lambda}_\alpha - \lambda_\alpha| \leq C_1 \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} + \frac{\log(1/\delta) \sqrt{\log n}}{\sqrt{k}} \right).$$

Proof. Let $\tilde{\alpha} > 0$. Then, we have that if $x \sim f$, then $\mathbb{P}(x \in H_{\tilde{\alpha}}(f)) = 1 - \tilde{\alpha}$. Thus, the probability that a sample point falls in $H_{\tilde{\alpha}}(f)$ is a Bernoulli random variable with probability $1 - \tilde{\alpha}$. Hence, by Hoeffding's inequality, we have that there exist constant $C' > 0$ such that

$$\mathbb{P} \left(1 - \tilde{\alpha} - C' \sqrt{\frac{\log(1/\delta)}{n}} \leq \frac{|H_{\tilde{\alpha}}(f) \cap X|}{n} \leq 1 - \tilde{\alpha} + C' \sqrt{\frac{\log(1/\delta)}{n}} \right) \geq 1 - \delta/4$$

Then it follows that choosing $\alpha_U := \alpha + C' \sqrt{\frac{\log(1/\delta)}{n}}$ we get

$$\mathbb{P} \left(\frac{|H_{\alpha_U}(f) \cap X|}{n} \leq 1 - \alpha \right) \geq 1 - \delta/4$$

Similarly, choosing $\alpha_L = \alpha - C' \sqrt{\frac{\log(1/\delta)}{n}}$ gives us

$$\mathbb{P} \left(\frac{|H_{\alpha_L}(f) \cap X|}{n} \geq 1 - \alpha \right) \geq 1 - \delta/4$$

Next, define

$$H_\alpha^{upper}(f) := \{x \in X : f_k(x) \geq \lambda_\alpha - \epsilon\}.$$

where $\epsilon > 0$ will be chosen later in order for $\widehat{H}_\alpha(f) \subseteq H_\alpha^{upper}(f)$. By Lemma 4, there exists $C_2, r_1 > 0$ depending on f such that for $\widehat{\epsilon} < r_1$ (which holds for n sufficiently large depending on f by Lemma 1), we have $\lambda_\alpha - C_2 \left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} \leq \lambda_{\alpha_L}$. As such, it suffices to choose ϵ such that for all $x \in \mathcal{X}$ such that if $f(x) \geq \lambda_\alpha - C_2 \left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D}$ then $f_k(x) \geq \lambda_\alpha - \epsilon$. This is because $\{x \in X : f_k(x) \geq \lambda_\alpha - \epsilon\}$ would contain $H_{\alpha_L}(f) \cap X$, which we showed earlier contains at least $1 - \alpha$ fraction of the samples. Define ϵ_0 such that $\epsilon = C_2 \left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} + \epsilon_0$. We have by Assumption 1,

$$\check{r}(x, \epsilon_0) \geq \left(\frac{1}{\check{C}_\beta} \left(\epsilon_0 + C_2 \left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} \right) \right)^{1/\beta} - \left(\frac{1}{\check{C}_\beta} \left(C_2 \left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} \right) \right)^{1/\beta}.$$

Then, there exists constant $C'' > 0$ sufficiently large depending on f such that if

$$\epsilon_0 \geq C'' \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} + \frac{\log(1/\delta)\sqrt{\log n}}{\sqrt{k}} \right)$$

then the conditions in Lemma 3 are satisfied for n sufficiently large. Thus, we have for all $x \in \mathcal{X}$ with $f(x) \geq \alpha - C_2 \left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D}$, then $f_k(x) \geq \alpha - \epsilon$. Hence, $\widehat{H}_\alpha(f) \subseteq H_\alpha^{upper}(f)$.

We now do the same in the other direction. Define

$$H_\alpha^{lower}(f) := \{x \in X : f_k(x) \geq \lambda_\alpha + \epsilon\}.$$

where ϵ will be chosen such that $H_\alpha^{lower}(f) \subseteq \widehat{H}_\alpha(f)$. By Lemma 4, it suffices to show that if $f_k(x) \geq \lambda_\alpha + \epsilon$ then $f(x) \geq \lambda_\alpha + C_2 \left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D}$. This direction follows a similar argument as the previous.

Thus, there exists a constant $C_1 > 0$ depending on f such that for n sufficiently large depending on f , we have:

$$|\widehat{\lambda}_\alpha - \lambda_\alpha| \leq C_1 \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} + \frac{\log(1/\delta)\sqrt{\log n}}{\sqrt{k}} \right),$$

as desired. \square

The next result bounds $\widehat{H}_\alpha(f)$ between two level sets of f .

Lemma 6. *Let $0 < \delta < 1$. There exists constant $C_1 > 0$ depending on f such that the following holds with probability at least $1 - \delta$ for n sufficiently large depending on f . Define*

$$H_\alpha^U(f) := \left\{ x \in \mathcal{X} : f(x) \geq \lambda_\alpha - C_1 \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} + \frac{\log(1/\delta)\sqrt{\log n}}{\sqrt{k}} \right) \right\}$$

$$H_\alpha^L(f) := \left\{ x \in \mathcal{X} : f(x) \geq \lambda_\alpha + C_1 \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} + \frac{\log(1/\delta)\sqrt{\log n}}{\sqrt{k}} \right) \right\}.$$

Then,

$$H_\alpha^L(f) \cap X \subseteq \widehat{H}_\alpha(f) \subseteq H_\alpha^U(f) \cap X.$$

Proof. To simplify notation, let us define the following:

$$K(n, k, \delta) := \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} + \frac{\log(1/\delta)\sqrt{\log n}}{\sqrt{k}} \right).$$

By Lemma 5, there exists $C_2 > 0$ such that defining

$$\begin{aligned} \widehat{H}_\alpha^U(f) &:= \{x \in X : f_k(x) \geq \lambda_\alpha - C_2 \cdot K(n, k, \delta)\} \\ \widehat{H}_\alpha^L(f) &:= \{x \in X : f_k(x) \geq \lambda_\alpha + C_2 \cdot K(n, k, \delta)\}, \end{aligned}$$

then we have

$$\widehat{H}_\alpha^L(f) \subseteq \widehat{H}_\alpha(f) \subseteq \widehat{H}_\alpha^U(f).$$

It suffices to show that there exists a constant $C_1 > 0$ such that

$$H_\alpha^L(f) \cap X \subseteq \widehat{H}_\alpha^L(f) \text{ and } \widehat{H}_\alpha^U(f) \subseteq H_\alpha^U(f) \cap X.$$

We start by showing $H_\alpha^L(f) \cap X \subseteq \widehat{H}_\alpha^L(f)$. To do this, show that for any $x \in \mathcal{X}$ satisfying $f(x) \geq \lambda_\alpha + C_1 \cdot K(n, k, \delta) + \epsilon$ satisfies $f_k(x) \geq \lambda_\alpha + C_1 \cdot K(n, k, \delta)$, where $\epsilon > 0$ will be chosen later. By a similar argument as in the proof of Lemma 5, we can choose $\epsilon \geq C' \cdot K(n, k, \delta)$ for some constant $C' > 0$ and the desired result holds for n sufficiently large. Similarly, there exists $C'' > 0$ such that $f_k(x) \leq \lambda_\alpha - (C_1 + C'') \cdot K(n, k, \delta)$ implies that $f(x) \leq \lambda_\alpha - C_1 \cdot K(n, k, \delta)$. The result follows by taking $C_2 = C_1 + \max\{C', C''\}$. \square

We are now ready to prove Theorem 5, a more general version of Theorem 1 which makes the dependence on δ explicit. Note that if $\delta = 1/n$, then $\log(1/\delta) = \log(n)$.

Theorem 5. [Extends Theorem 1] Let $0 < \delta < 1$ and suppose that f is continuous and has compact support $\mathcal{X} \subseteq \mathbb{R}^D$ and satisfies Assumption 1. There exists constants $C_l, C_u, C > 0$ depending on f such that the following holds with probability at least $1 - \delta$. Suppose that k satisfies

$$C_l \cdot \log(1/\delta)^2 \cdot \log n \leq k \leq C_u \cdot \log(1/\delta)^{2D/(2\beta+D)} \cdot (\log n)^{D(2\beta+D)} \cdot n^{2\beta/(2\beta+D)}$$

then we have

$$d_H(H_\alpha(f), \widehat{H}_\alpha(f)) \leq C \cdot \left(\log(1/\delta)^{1/2D} \cdot n^{-1/2D} + \log(1/\delta)^{1/\beta} \cdot \log(n)^{1/2\beta} \cdot k^{-1/2\beta} \right).$$

Proof of Theorem 5. Again, to simplify notation, let us define the following:

$$K(n, k, \delta) := \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/D} + \frac{\log(1/\delta)\sqrt{\log n}}{\sqrt{k}} \right).$$

There are two directions to show for Hausdorff distance result. That (1) $\max_{x \in \widehat{H}_\alpha(f)} d(x, H_\alpha(f))$ is bounded, that is none of the high-density points recovered by Algorithm 1 are far from the true high-density region; and (2) that $\sup_{x \in H_\alpha(f)} d(x, \widehat{H}_\alpha(f))$ is bounded, that Algorithm 1 recovers a good covering of the entire high-density region.

We first show (1). By Lemma 6, we have that there exist $C_1 > 0$ such that

$$H_\alpha^U(f) := \{x \in \mathcal{X} : f(x) \geq \lambda_\alpha - C_1 K(n, k, \delta)\}$$

contains $\widehat{H}_\alpha(f)$. Thus,

$$\max_{x \in \widehat{H}_\alpha(f)} d(x, H_\alpha(f)) \leq \sup_{x \in H_\alpha^U(f)} d(x, H_\alpha(f)) \leq \left(C_1 \cdot K(n, k, \delta) \cdot \frac{1}{\bar{C}_\beta} \right)^{1/\beta}$$

where the second inequality holds by Assumption 1. Now for the other direction, we have by Triangle inequality that

$$\sup_{x \in H_\alpha(f)} d(x, \widehat{H}_\alpha(f)) \leq \sup_{x \in H_\alpha(f)} d(x, H_\alpha^L(f)) + \sup_{x \in H_\alpha^L(f)} d(x, \widehat{H}_\alpha(f)).$$

The first term can be bounded by using Assumption 1.

$$\sup_{x \in H_\alpha^L(f)} d(x, H_\alpha^L(f)) \leq \left(C_1 \cdot K(n, k, \delta) \cdot \frac{1}{\bar{C}_\beta} \right)^{1/\beta}.$$

Now for the second term, we see that by Lemma 6, $\widehat{H}_\alpha(f)$ contains all of the sample points of $H_\alpha^L(f)$. Thus, we have

$$\sup_{x \in H_\alpha^L(f)} d(x, \widehat{H}_\alpha(f)) \leq \sup_{x \in H_\alpha^L(f)} d(x, H_\alpha^L(f) \cap X)$$

By Assumption 1, for $r < r_0$, and $x \in H_\alpha^L(f)$ we have $\mathcal{F}(B(x, r)) \geq \rho r^D$, where \mathcal{F} is the distribution corresponding to f . Choosing $r \geq \left(\frac{C_{\delta, n}}{\rho} \frac{\sqrt{D \log n}}{n} \right)^{1/D}$ gives us that by Lemma 1 that $\mathcal{F}_n(B(x, r)) > 0$ where \mathcal{F}_n is the distribution of X and thus, we have

$$\sup_{x \in H_\alpha^L(f)} d(x, H_\alpha^L(f) \cap X) \leq \left(\frac{C_{\delta, n}}{\rho} \frac{\sqrt{D \log n}}{n} \right)^{1/D},$$

which is dominated by the error contributed by the other error and the result follows. \square

C Supporting results for Theorem 2 Proof

In this section, we note that we will reuse some notation from the last section for the manifold case.

Lemma 7 (Manifold Version of Uniform convergence of empirical Euclidean balls (Lemma 7 of [1])). *Let \mathcal{F} be the true distribution and \mathcal{F}_n be the empirical distribution w.r.t. sample X . Let \mathcal{N} be a minimal fixed set such that each point in M is at most distance $1/n$ from some point in \mathcal{N} . There exists a universal constant C_0 such that the following holds with probability at least $1 - \delta$. For all $x \in X \cup \mathcal{N}$,*

$$\begin{aligned} \mathcal{F}(B) &\geq C_{\delta, n} \frac{\sqrt{d \log n}}{n} \Rightarrow \mathcal{F}_n(B) > 0 \\ \mathcal{F}(B) &\geq \frac{k}{n} + C_{\delta, n} \frac{\sqrt{k}}{n} \Rightarrow \mathcal{F}_n(B) \geq \frac{k}{n} \\ \mathcal{F}(B) &\leq \frac{k}{n} - C_{\delta, n} \frac{\sqrt{k}}{n} \Rightarrow \mathcal{F}_n(B) < \frac{k}{n}. \end{aligned}$$

where $C_{\delta, n} = C_0 \log(2/\delta) \sqrt{d \log n}$, \mathcal{F}_n is the empirical distribution, and $k \geq C_{\delta, n}$.

Definition 5 (k-NN Density Estimator on Manifold).

$$f_k(x) := \frac{k}{n \cdot v_d \cdot r_k(x)^d}.$$

Lemma 8 (Manifold version of f_k upper bound [27]). *Define the following which characterizes how much the density increases locally in M :*

$$\hat{r}(\epsilon, x) := \sup \left\{ r : \sup_{x' \in B(x, r) \cap M} f(x') - f(x) \leq \epsilon \right\}.$$

Fix $\lambda_0 > 0$ and $\delta > 0$ and suppose that $k \geq C_{\delta, n}^2$. Then there exists constant $C_1 \equiv C_1(\lambda_0, d, \tau)$ such that if

$$k \leq C_1 \cdot C_{\delta, n}^{2d/(2+d)} \cdot n^{2/(2+d)},$$

then the following holds with probability at least $1 - \delta$ uniformly in $\epsilon > 0$ and $x \in X$ with $f(x) + \epsilon \geq \lambda_0$:

$$f_k(x) < \left(1 + 3 \cdot \frac{C_{\delta, n}}{\sqrt{k}} \right) \cdot (f(x) + \epsilon),$$

provided k satisfies $v_d \cdot \hat{r}(\epsilon, x)^d \cdot (f(x) + \epsilon) \geq \frac{k}{n} - C_{\delta, n} \frac{\sqrt{k}}{n}$.

Lemma 9 (Manifold version of f_k lower bound [27]). *Define the following which characterizes how much the density decreases locally in M :*

$$\check{r}(\epsilon, x) := \sup \left\{ r : \sup_{x' \in B(x, r) \cap M} f(x) - f(x') \leq \epsilon \right\}.$$

Fix $\lambda_0 > 0$ and $0 < \delta < 1$ and suppose $k \geq C_{\delta, n}$. Then there exists constant $C_2 \equiv C_2(\lambda_0, d, \tau)$ such that if

$$k \leq C_2 \cdot C_{\delta, n}^{2d/(4+d)} \cdot n^{4/(4+d)},$$

then with probability at least $1 - \delta$, the following holds uniformly for all $\epsilon > 0$ and $x \in X$ with $f(x) - \epsilon \geq \lambda_0$:

$$f_k(x) \geq \left(1 - 3 \cdot \frac{C_{\delta, n}}{\sqrt{k}}\right) \cdot (f(x) - \epsilon),$$

provided k satisfies $v_d \cdot \check{r}(\epsilon, x)^d \cdot (f(x) - \epsilon) \geq \frac{4}{3} \left(\frac{k}{n} + C_{\delta, n} \frac{\sqrt{k}}{n}\right)$.

D Proof of Theorem 2

The proof essentially follows the same structure as the full-dimensional case, with primary difference in the density estimation bounds.

Lemma 10 (Manifold Version of Lemma 4). *There exists a constants $C_1, r_1 > 0$ depending on f such that the following holds for all $0 < \epsilon < r_1$ such that*

$$0 < \lambda_\alpha - \lambda_{\alpha-\epsilon} \leq C_1 \epsilon^{\beta/d} \text{ and } 0 < \lambda_{\alpha+\epsilon} - \lambda_\alpha \leq C_1 \epsilon^{\beta/d}$$

Proof. The proof follows the same structure as the proof of Lemma 4, with the difference being the change in dimension, and is omitted here. \square

Lemma 11 (Manifold Version of Lemma 5). *Let $0 < \delta < 1$. Let $\hat{\epsilon}$ be the ϵ setting chosen by Algorithm 1 after the binary search procedure. Define*

$$\widehat{\lambda}_\alpha := \frac{k}{v_D \cdot n \cdot \hat{\epsilon}^d}.$$

Then, with probability at least $1 - \delta$, we have there exist constant $C_1 > 0$ depending on f and M such that for n sufficiently large depending on f and M , we have

$$|\widehat{\lambda}_\alpha - \lambda_\alpha| \leq C_1 \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/d} + \frac{\log(1/\delta) \sqrt{\log n}}{\sqrt{k}} \right).$$

Proof. The proof is essentially the same as that of Lemma 5. The only difference is that instead of applying the full-dimensional versions of the uniform k -NN density estimate bounds (Lemma 2 and 3), we instead apply the manifold analogues (Lemma 8 and 9). Besides from constant factors, the major difference is in the allowable range for k . In the full-dimensional case, we only need $k \lesssim n^{2\beta/(2\beta+d)}$ for the density estimation bounds to hold. However, here we require $k \lesssim \min\{n^{2/(2+d)}, n^{2\beta/(2\beta+d)}\} = n^{2 \max\{1, \beta\}/(2\beta'+d)}$. \square

Lemma 12 (Manifold Version of Lemma 5). *Let $0 < \delta < 1$. There exists constant $C_1 > 0$ depending on f and M such that the following holds with probability at least $1 - \delta$ for n sufficiently large depending on f and M . Define*

$$H_\alpha^U(f) := \left\{ x \in \mathcal{X} : f(x) \geq \lambda_\alpha - C_1 \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/d} + \frac{\log(1/\delta) \sqrt{\log n}}{\sqrt{k}} \right) \right\}$$

$$H_\alpha^L(f) := \left\{ x \in \mathcal{X} : f(x) \geq \lambda_\alpha + C_1 \left(\left(\sqrt{\frac{\log(1/\delta)}{n}} \right)^{\beta/d} + \frac{\log(1/\delta) \sqrt{\log n}}{\sqrt{k}} \right) \right\}.$$

Then,

$$H_\alpha^L(f) \cap X \subseteq \widehat{H}_\alpha(f) \subseteq H_\alpha^U(f) \cap X.$$

Proof. Same comment as the proof for Lemma 11. \square

Theorem 6. [Extends Theorem 2] Let $0 < \delta < 1$. Suppose that density function f is continuous and supported on M and Assumptions 1 and 2 hold. Suppose also that there exists $\lambda_0 > 0$ such that $f(x) \geq \lambda_0$ for all $x \in M$. Then, there exists constants $C_l, C_u, C > 0$ depending on f such that the following holds with probability at least $1 - \delta$. Suppose that k satisfies

$$C_l \cdot \log(1/\delta)^2 \cdot \log n \leq k \leq C_u \cdot \log(1/\delta)^{2d/(2\beta'+d)} \cdot (\log n)^{d(2\beta'+d)} \cdot n^{2\beta'/(2\beta'+d)}$$

where $\beta' := \max\{1, \beta\}$. Then we have

$$d_H(H_\alpha(f), \widehat{H}_\alpha(f)) \leq C \cdot \left(\log(1/\delta)^{1/2d} \cdot n^{-1/2d} + \log(1/\delta)^{1/\beta} \cdot \log(n)^{1/2\beta} \cdot k^{-1/2\beta} \right).$$

Proof of Theorem 6. Proof is the same as the full-dimensional case given the contributed Lemmas of this section and is omitted here. \square

E Supporting Results for Theorem 3 Proof

Next, we need the following on the volume of the intersection Euclidean ball and M ; this is required to get a handle on the true mass of the ball under \mathcal{F}_M in later arguments. The upper and lower bounds follow from [4] and Lemma 5.3 of [36]. The proof can be found e.g. in [27].

Lemma 13 (Ball Volume). If $0 < r < \min\{\tau/4d, 1/\tau\}$, and $x \in M$ then

$$v_d r^d (1 - \tau^2 r^2) \leq \text{vol}_d(B(x, r) \cap M) \leq v_d r^d (1 + 4dr/\tau).$$

where v_d is the volume of a unit ball in \mathbb{R}^d and vol_d is the volume w.r.t. the uniform measure on M .

The next is a bound uniform convergence of balls:

Lemma 14 (Lemma 3 of [28]). Let \mathcal{B} be the set of all balls in \mathbb{R}^D , \mathcal{F} is some distribution and \mathcal{F}_n is an empirical distribution. With probability at least $1 - \delta$, the following holds uniformly for every $B \in \mathcal{B}$ and $\gamma \geq 0$:

$$\begin{aligned} \mathcal{F}(B) \geq \gamma &\Rightarrow \mathcal{F}_n(B) \geq \gamma - \beta_n \sqrt{\gamma} - \beta_n^2, \\ \mathcal{F}(B) \leq \gamma &\Rightarrow \mathcal{F}_n(B) \leq \gamma + \beta_n \sqrt{\gamma} + \beta_n^2, \end{aligned}$$

where $\beta_n = 8d \log(1/\delta) \sqrt{\log n/n}$.

F Proof of Theorem 3

The first result says that within the manifold, the vast majority of the probability mass is attributed to the manifold distributions.

Lemma 15. There exists $C_1, r_1 > 0$ depending on $\mathcal{F}_M, \mathcal{F}_E, M$ such that the following holds uniformly over $x \in M$ and $0 < r < r_1$.

$$\frac{\mathcal{F}_E(B(x, r))}{\mathcal{F}_M(B(x, r))} \leq C_1 \cdot r^{D-d}.$$

Proof. Let $x \in M$ and $r > 0$. We have

$$\mathcal{F}_M(B(x, r)) \geq \lambda_0 \cdot \text{vol}_d(B(x, r) \cap M) \geq v_d r^d (1 - \tau^2 r^2) \cdot \lambda_0.$$

where the second inequality holds by Lemma 13 for r sufficiently small. On the other hand, we have

$$\mathcal{F}_E(B(x, r)) \leq \|f_E\|_\infty v_D r^D.$$

Thus, we have there exists $C_1 > 0$ depending on f_M, M , and f_E such that

$$\frac{\mathcal{F}_E(B(x, r))}{\mathcal{F}_M(B(x, r))} \leq C_1 \cdot r^{D-d},$$

as desired. \square

We next show that points far away from $H_{\tilde{\alpha}}(f_M)$ do not get selected as high-density points by Algorithm 1.

Lemma 16. *There exists $\omega_0 > 0$ such that for any $0 < \omega < \omega_0$ and n sufficiently large depending on $\mathcal{F}_M, \mathcal{F}_E, M$ and ω , with probability at least $1 - \delta$, Algorithm 1 will not select any points outside of $H_{\tilde{\alpha}-\omega}(f_M)$.*

Proof. By Assumption 1, we can choose ω sufficiently small so that for the density f_M , $|\lambda_{\tilde{\alpha}-\omega} - \lambda_{\tilde{\alpha}}| \leq \tilde{C}_\beta \cdot (r_c/3)^\beta$. Then, at the $(\tilde{\alpha}-\omega)$ -density level, we will be within the area where the regularity assumptions hold.

Next, by Hoeffding's inequality, we have that there exist constant $C' > 0$ such that for $\bar{\alpha} > 0$:

$$\mathbb{P} \left(1 - \bar{\alpha} - C' \sqrt{\frac{\log(1/\delta)}{n}} \leq \frac{|H_{\frac{\bar{\alpha}-\eta}{1-\eta}}(f_M) \cap X|}{n} \leq 1 - \bar{\alpha} + C' \sqrt{\frac{\log(1/\delta)}{n}} \right) \geq 1 - \delta/3.$$

Choosing $\bar{\alpha} = \alpha - C' \sqrt{\frac{\log(1/\delta)}{n}}$, then it follows that with probability at least $1 - \delta/3$,

$$H_0 := H_{\tilde{\alpha}-C' \sqrt{\log(1/\delta)/(\sqrt{n} \cdot (1-\eta))}}(f_M)$$

satisfies $|H_0 \cap X| > (1 - \alpha) \cdot n$. Now, defining

$$H_\omega := H_{\tilde{\alpha}-\omega}(f_M)$$

Let r be the value of ε used by Algorithm 1. Now, it suffices to show that for n sufficiently large depending on f_M :

$$\max_{x \in X \setminus H_\omega} \mathcal{F}_n(B(x, r)) < \min_{x \in H_0} \mathcal{F}_n(B(x, r)).$$

where \mathcal{F}_n is the empirical distribution. This is because Algorithm 1 filters out sample points whose ε -ball has less than k sample points for its final ε value, which is the value which allows it to filter α -fraction of the points.

By Lemma 15, it suffices to show that

$$\max_{x \in X \setminus H_\omega} \mathcal{F}_{M,n}(B(x, r)) (1 + C_1 r^{D-d}) < \min_{x \in H_0} \mathcal{F}_{M,n}(B(x, r)) (1 - C_1 r^{D-d}).$$

where $\mathcal{F}_{M,n}(A)$ denote the fraction of samples drawn from \mathcal{F}_M which lie in A w.r.t. our entire sample X .

Then, by Lemma 14, it will be enough to show that

$$\begin{aligned} & \max_{x \in X \setminus H_\omega} (\mathcal{F}_M(B(x, r)) + \beta_n \sqrt{\mathcal{F}_M(B(x, r))} + \beta_n^2) (1 + C_1 r^{D-d}) \\ & < \min_{x \in H_0} (\mathcal{F}_M(B(x, r)) - \beta_n \sqrt{\mathcal{F}_M(B(x, r))} - \beta_n^2) (1 - C_1 r^{D-d}). \end{aligned}$$

where $\beta_n = 8d \log(1/\delta) \sqrt{\log n/n}$.

To bound the LHS, we have by Lemma 13

$$\begin{aligned} & \max_{x \in X \setminus H_\omega} (\mathcal{F}_M(B(x, r)) + \beta_n \cdot \sqrt{\mathcal{F}_M(B(x, r))} + \beta_n^2) (1 + C_1 r^{D-d}) \\ & \leq \max_{x \in X \setminus H_\omega} \left\{ \left(\inf_{x' \in B(x, r)} f_M(x') \right) \cdot \left(1 + \beta_n / \sqrt{\|f_M\|_\infty} + \beta_n^2 / \|f_M\|_\infty \right) (1 + C_1 r^{D-d}) (1 + 4dr/\tau) \right\} \\ & \leq \max_{x \in X \setminus H_\omega} \left\{ \left(\inf_{x' \in B(x, r)} f_M(x') \right) (1 + C_2 \beta_n + C_3 r) \right\} \\ & \leq (\lambda_{\tilde{\alpha}-\omega} + \iota(f_M, r)) (1 + C_2 \beta_n + C_3 r) \end{aligned}$$

for some $C_2, C_3 > 0$ and ι is the modulus of continuity, that is $\iota(f_M, r) := \sup_{x, x' \in M: |x-x'| \leq r} |f_M(x) - f_M(x')|$ (i.e. f_M is uniformly continuous since it is continuous over a compact support, so $\iota(f_M, r) \rightarrow 0$ as $r \rightarrow 0$).

Similarly, for the RHS, we can show for some constants C_4, C_5 that

$$\begin{aligned} & \min_{x \in H_0} (\mathcal{F}_M(B(x, r)) - \beta_n \sqrt{\mathcal{F}_M(B(x, r)) - \beta_n^2}) (1 - C_1 r^{D-d}) \\ & \geq (\lambda_{\tilde{\alpha}-C' \sqrt{\log(1/\delta)}/(\sqrt{n}(1-\eta))} - \iota(f_M, r)) (1 - C_4 \beta_n - C_5 r) \end{aligned}$$

The result follows since $r \rightarrow 0$ as $n \rightarrow \infty$ (since by Lemma 1, r is a k -NN radius so $r \lesssim (k/n)^{1/D} \rightarrow 0$ given the conditions on k of Theorem 3) and the fact that $\lambda_{\tilde{\alpha}-\omega} < \lambda_{\tilde{\alpha}-C' \sqrt{\log(1/\delta)}/\sqrt{n}}$ for n sufficiently large. As desired. \square

Lemma 17 (Bounding density estimators w.r.t to entire sample vs w.r.t. samples on manifold). *For $x \in \mathbb{R}^D$, define the following:*

$$\begin{aligned} r_k(x) &:= \inf\{\epsilon > 0 : |B(x, \epsilon) \cap X| \geq k\} \\ \tilde{r}_k(x) &:= \inf\{\epsilon > 0 : |B(x, \epsilon) \cap X \cap M| \geq k\} \end{aligned}$$

where the former is simply the k -NN radius we've been using thus far and the latter is the k -NN radius if we were to restrict the samples to only those that came from M . Then likewise, define the analogous density estimators:

$$f_k(x) := \frac{k}{n \cdot v_d \cdot r_k(x)^d} \quad \text{and} \quad \tilde{f}_k(x) := \frac{k}{n \cdot v_d \cdot \tilde{r}_k(x)^d}$$

where again, the former is the usual k -NN density estimator on manifolds. Then, there exists C_1 such that the following holds with high probability.

$$\sup_{x \in M} |f_k(x) - \tilde{f}_k(x)| \leq C_1 \cdot (k/n)^{D/d-1}.$$

Proof. By Lemma 14, there exists $C_2 > 0$ depending on \mathcal{F} and \mathcal{F}_M such that

$$\mathcal{F}_n(B(x, r_k(x))) = k \Rightarrow |\mathcal{F}(B(x, r_k(x))) - k| \leq C_2 \beta_n$$

and

$$\mathcal{F}_{M,n}(B(x, \tilde{r}_k(x))) = k \Rightarrow |\mathcal{F}_M(B(x, \tilde{r}_k(x))) - k| \leq C_2 \beta_n,$$

where $\mathcal{F}_{M,n}$ is the empirical distribution w.r.t. $X \cap M$. Next, by Lemma 15, we have for some constant $C_3 > 0$:

$$\begin{aligned} \mathcal{F}(B(x, \tilde{r}_k(x))) &\leq \mathcal{F}_M(B(x, \tilde{r}_k(x))) (1 + C_3 \tilde{r}_k(x)^{D-d}) \\ &\leq (k + C_2 \beta_n) (1 + C_3 \cdot \tilde{r}_k(x)^{D-d}) \\ &\leq (k + C_2 \beta_n) (1 + C_4 \cdot (k/n)^{D/d-1}) \\ &\leq k \cdot (1 + C_5 (k/n)^{D/d-1}). \end{aligned}$$

where the second last inequality holds for some constant $C_4 > 0$ by Lemma 7 and $C_5 > 0$ is some constant depending on \mathcal{F} and \mathcal{F}_M and M . Then it follows that for some constant $C_6 > 0$, we have

$$\frac{\mathcal{F}(B(x, \tilde{r}_k(x)))}{\mathcal{F}(B(x, r_k(x)))} \leq 1 + C_6 (k/n)^{D/d-1}.$$

In the other direction, we trivially have $\tilde{r}_k(x) \geq r_k(x)$, so

$$1 \leq \frac{\mathcal{F}(B(x, \tilde{r}_k(x)))}{\mathcal{F}(B(x, r_k(x)))} \leq 1 + C_6 (k/n)^{D/d-1}.$$

The result follows. \square

Theorem 7. [Extends Theorem 3] *Let $0 < \eta < \alpha < 1$ and $0 < \delta < 1$. Suppose that distribution \mathcal{F} is a weighted mixture $(1 - \eta) \cdot \mathcal{F}_M + \eta \cdot \mathcal{F}_E$ where \mathcal{F}_M is a distribution with continuous density f_M supported on a d -dimensional manifold M satisfying Assumption 2 and \mathcal{F}_E is a (noise) distribution with continuous density f_E with compact support over \mathbb{R}^D with $d < D$. Suppose also that there exists $\lambda_0 > 0$ such that $f_M(x) \geq \lambda_0$ for all $x \in M$ and $H_{\tilde{\alpha}}(f_M)$ (where $\tilde{\alpha} := \frac{\alpha-\eta}{1-\eta}$) satisfies Assumption 1 for density f_M . Let \hat{H}_α be the output of Algorithm 1 on a sample X of size n drawn i.i.d. from \mathcal{F} .*

Then, there exists constants $C_l, C_u, C > 0$ depending on f_M, f_E, η, M such that the following holds with probability at least $1 - \delta$. Suppose that k satisfies

$$C_l \cdot \log(1/\delta)^2 \cdot \log n \leq k \leq C_u \cdot \log(1/\delta)^{2d/(2\beta'+d)} \cdot (\log n)^{d(2\beta'+d)} \cdot n^{2\beta'/(2\beta'+d)}$$

where $\beta' := \max\{1, \beta\}$. Then we have

$$d_H(H_{\tilde{\alpha}}(f_M), \widehat{H}_{\alpha}) \leq C \cdot \left(\log(1/\delta)^{1/2d} \cdot n^{-1/2d} + \log(1/\delta)^{1/\beta} \cdot \log(n)^{1/2\beta} \cdot k^{-1/2\beta} \right).$$

Proof of Theorem 7. The proof follows in a similar way as that of Theorem 6, except with the complexity of having added full-dimensional noise. We will only highlight the difference and provide a sketch of the proof here.

Lemma 16 and 17 give us a handle on the additional complexity when having separate noise distribution, compared to the earlier manifold setting of Theorem 2.

Lemma 16 guarantees that the points in \widehat{H}_{α} lie in the inside of M with margin. In particular, that means the noise points are filtered out by the algorithm and thus, we are reduced to reasoning about the $\tilde{\alpha}$ -high-density-set of f_M .

Then, Lemma 17 ensures that the k -NN density estimator used for our analysis for the entire sample X is actually quite close to the k -NN density estimator with respect to $M \cap X$ within M . In other words, we can use the k -NN density estimator to estimate f_M without knowing which samples of X were in M . Lemma 17 shows that the additional error in density estimation we obtain is $\approx (k/n)^{D/d-1} \lesssim (k/n)^{1/d} \lesssim (\log n)/\sqrt{k}$, where the first inequality holds since $D > d$ and the latter holds from the conditions on k . It turns out that this error term can be absorbed as a constant in the previous result of Theorem 6. \square

G Proof of Theorem 4

Proof of Theorem 4. For the first inequality, we have

$$\xi(h, x) \geq \frac{d(x, M_{\tilde{h}(x)}) - \epsilon_n}{d(x, M_{h(x)}) + \epsilon_n} = \frac{d(x, M_{\tilde{h}(x)})}{d(x, M_{h(x)})} - \frac{\epsilon_n}{d(x, M_{h(x)}) + \epsilon_n} \cdot \left(\frac{d(x, M_{\tilde{h}(x)})}{d(x, M_{h(x)})} + 1 \right),$$

where the first inequality holds by Theorem 3. This implies that

$$\frac{d(x, M_{\tilde{h}(x)})}{d(x, M_{h(x)})} < 1 - \gamma,$$

which implies that $h(x) \neq h^*(x)$. For the second inequality, we have

$$\frac{1}{\xi(h, x)} \geq \frac{d(x, M_{h(x)}) - \epsilon_n}{d(x, M_{\tilde{h}(x)}) + \epsilon_n} = \frac{d(x, M_{h(x)})}{d(x, M_{\tilde{h}(x)})} - \frac{\epsilon_n}{d(x, M_{\tilde{h}(x)}) + \epsilon_n} \cdot \left(\frac{d(x, M_{h(x)})}{d(x, M_{\tilde{h}(x)})} + 1 \right)$$

where the first inequality holds by Theorem 3. Thus, if the condition of the theorem statement holds, then

$$\frac{d(x, M_{h(x)})}{d(x, M_{\tilde{h}(x)})} < 1 - \gamma \Rightarrow \frac{d(x, M_{h(x)})}{d(x, M_c)} < 1 - \gamma$$

for all $c \neq h(x)$, which implies that $h(x) = h^*(x)$ \square

H Experimental details

We used 44k training images, and 11k testing images for MNIST data set. For ImageNet, we sampled 20 classes from InceptionV3 model [45], and used 10,000 images to train our methods and tested on 4000 images. In both MNIST and ImageNet, we reduced dimension of the input data using PCA with 20 components.

MNIST model contained two sets of a convolutional layer followed by a fully connected layer. The details of InceptionV3 model can be found from [45]. We conduct crossvalidation to find α parameter.

I Additional UCI Experiments

I.1 When to trust: Precision for correct predictions by percentile

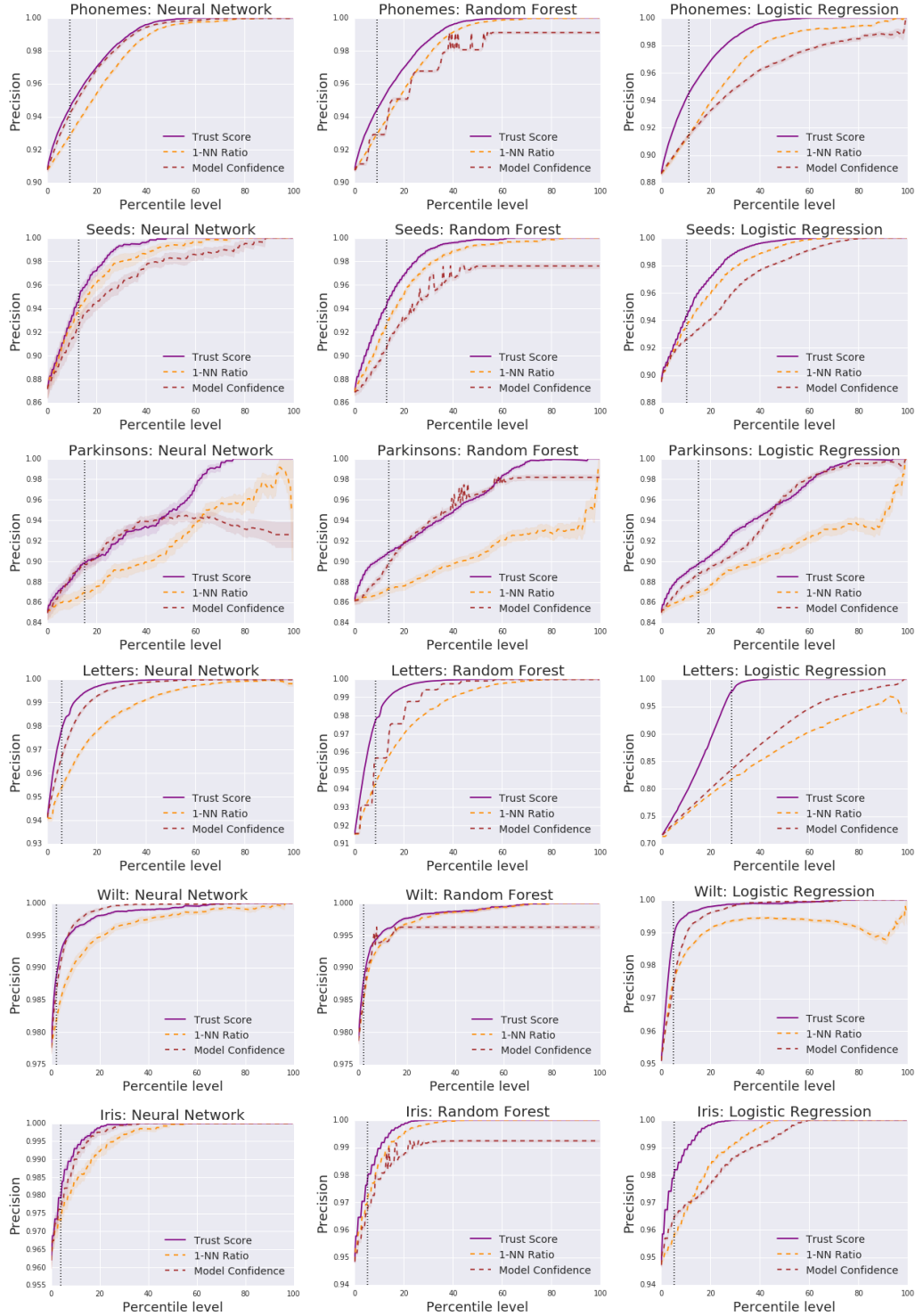


Figure 5: UCI data sets and precision on correctness

I.2 When to not trust: Precision for misclassification predictions by percentile

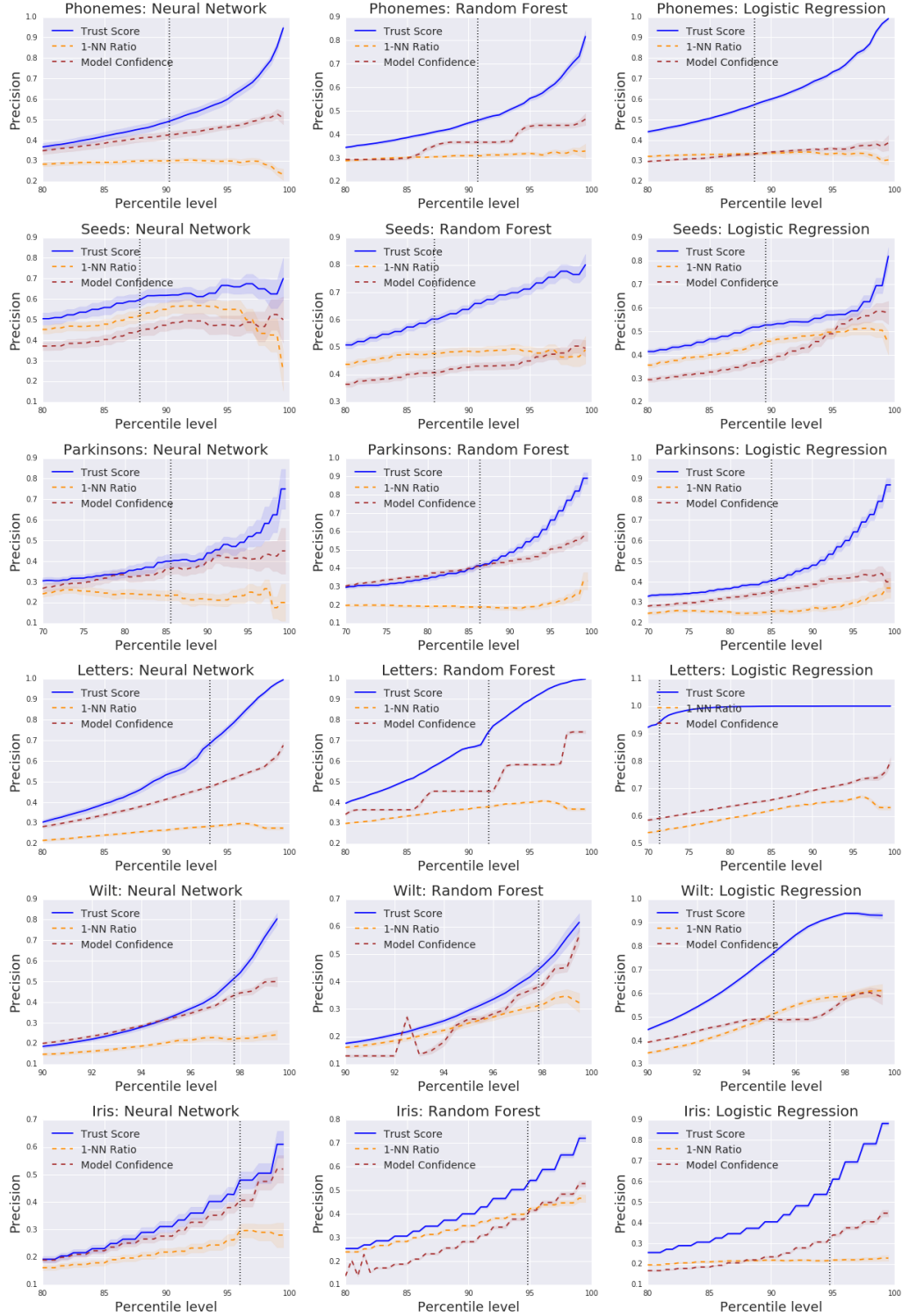
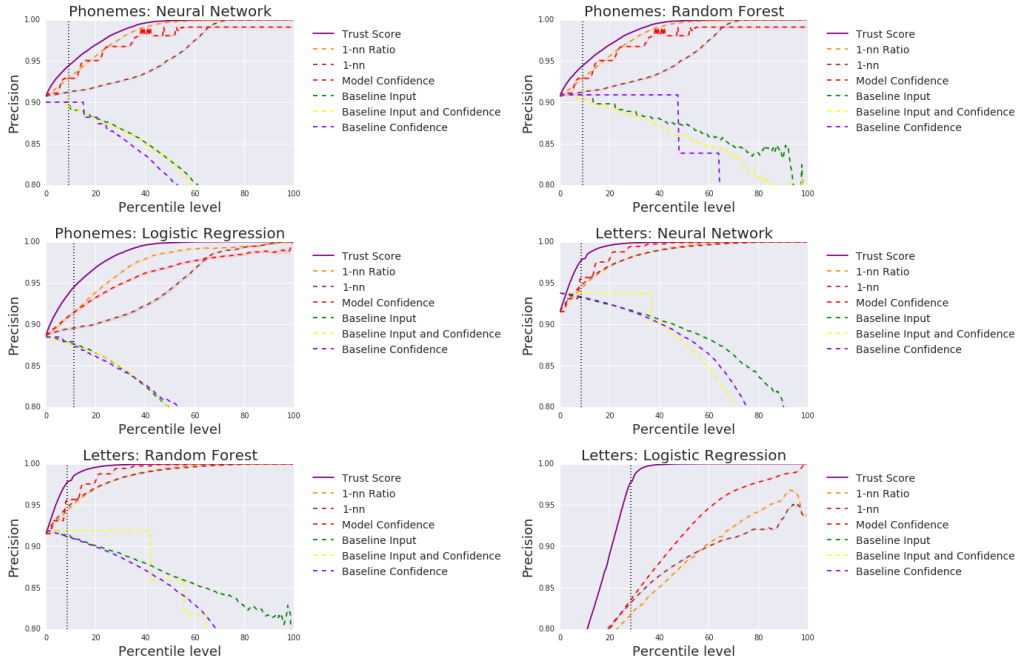
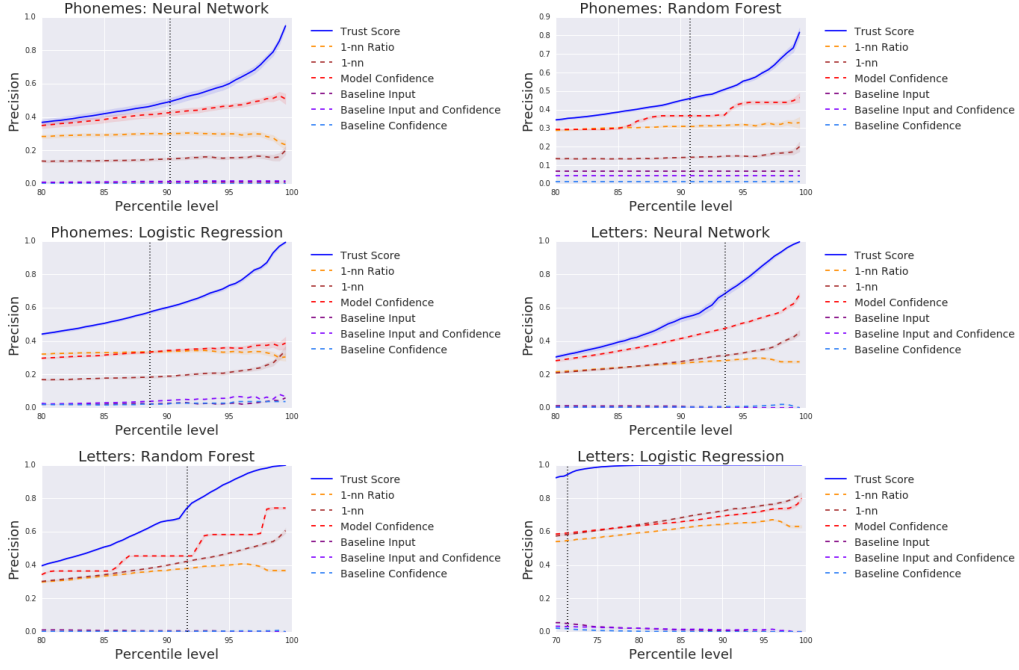


Figure 6: UCI data sets and precision on incorrectness

J Additional baselines



K Full experiment figures for MNIST and InceptionV3

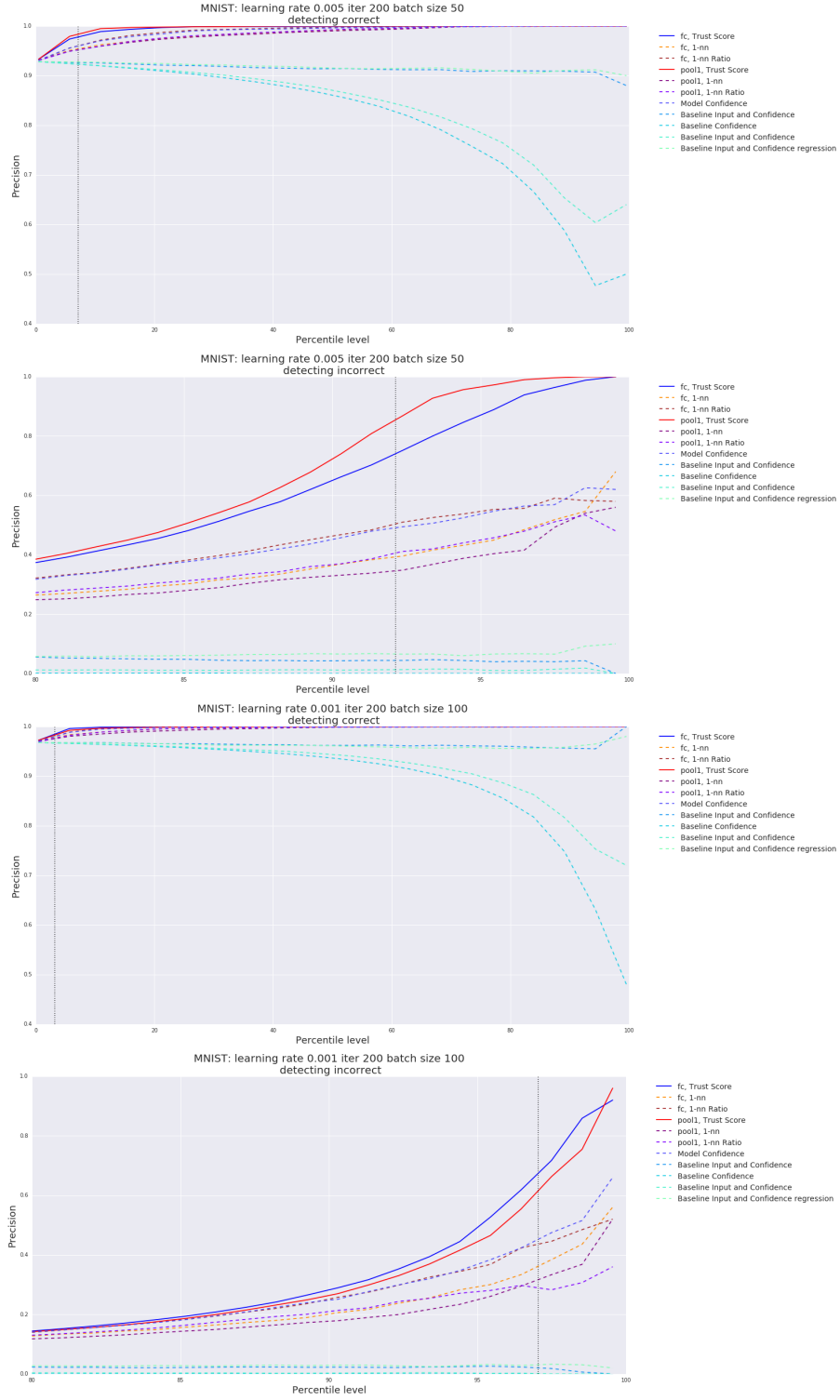


Figure 7: MNIST full results

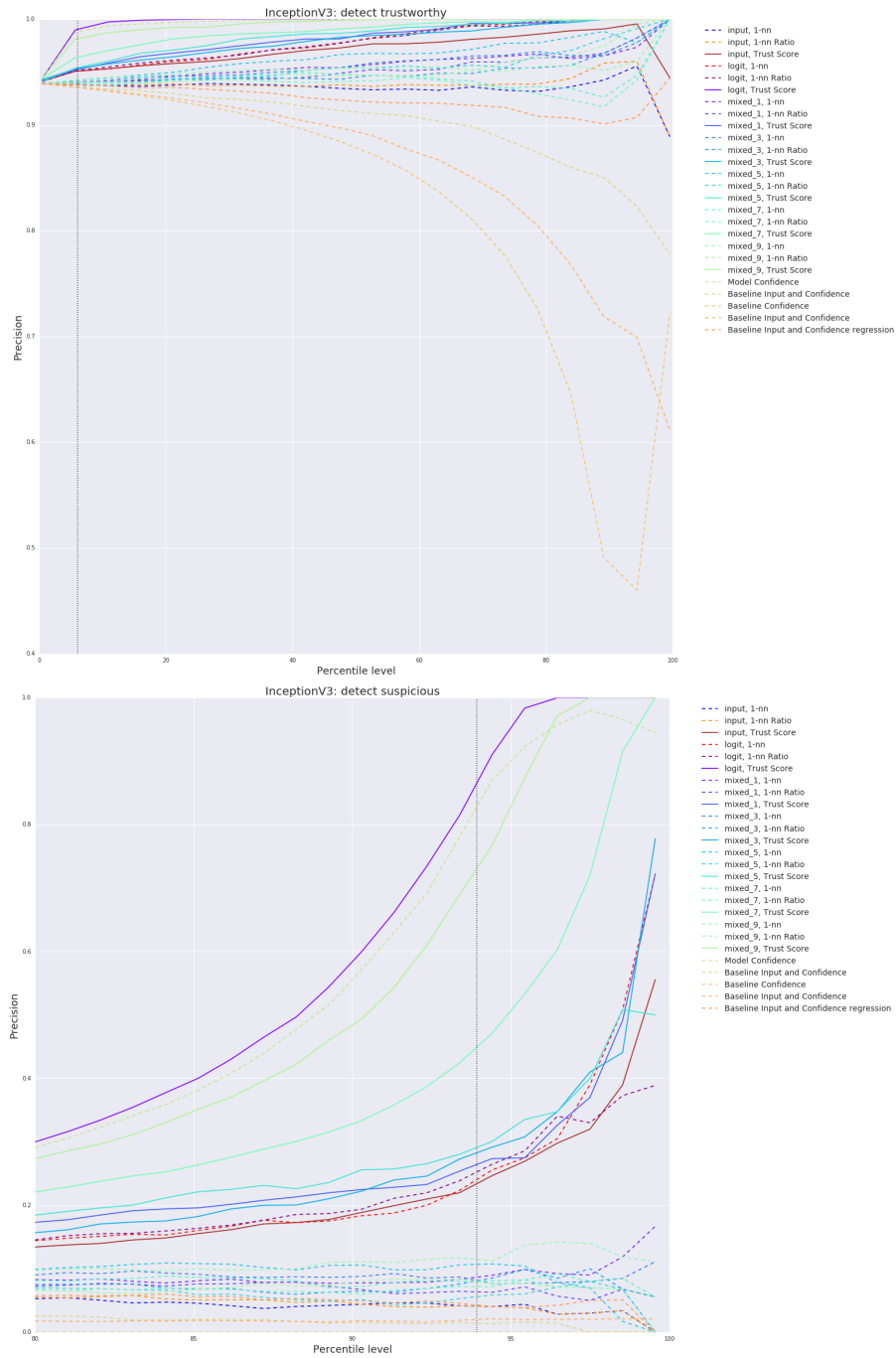


Figure 8: InceptionV3 full results

L Bigger figures for MNIST and InceptionV3 from main manuscript

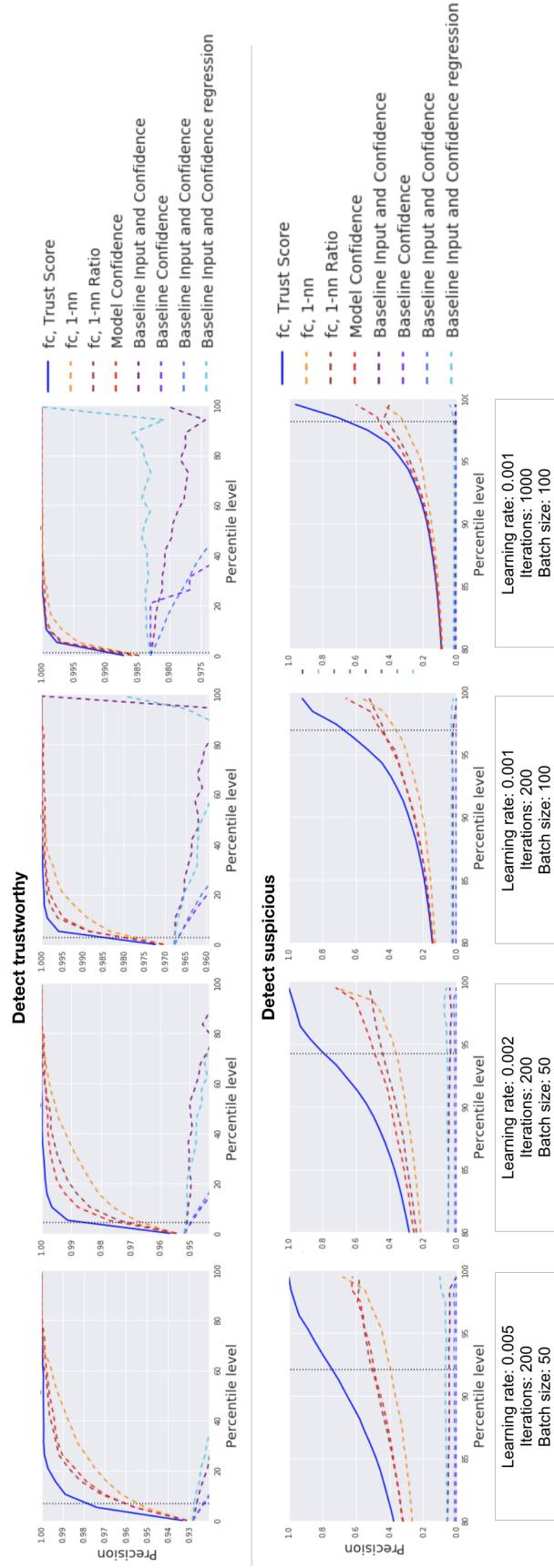


Figure 9: MNIST: Three different models (each column) as well as precision on identifying correctly classified (top) and incorrectly classified (bottom) examples. The baselines' curves have a widening gap compared to our methods when model achieves lower accuracy. The accuracy level of the neural network (indicated by the vertical dotted black lines) increase from left to right. "fc" is a fully-connected layer in the network.

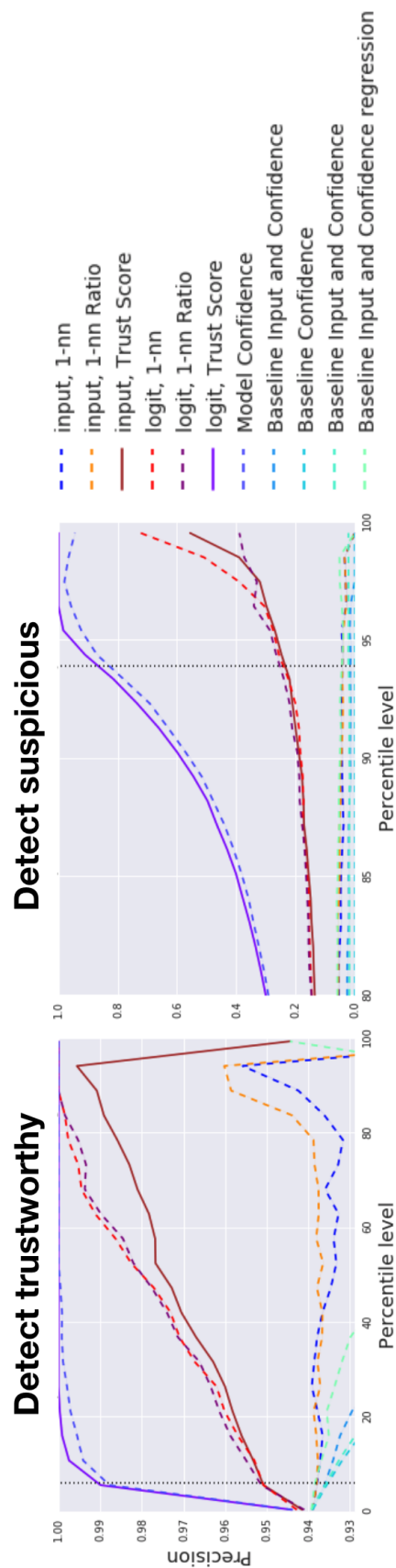


Figure 10: InceptionV3: precision on correct (left) and incorrect (right) precision. The black dotted line represents 1-accuracy (left) and accuracy (right). In general, our method returns higher performance with deeper layers (closer to logit) than with lower layers.

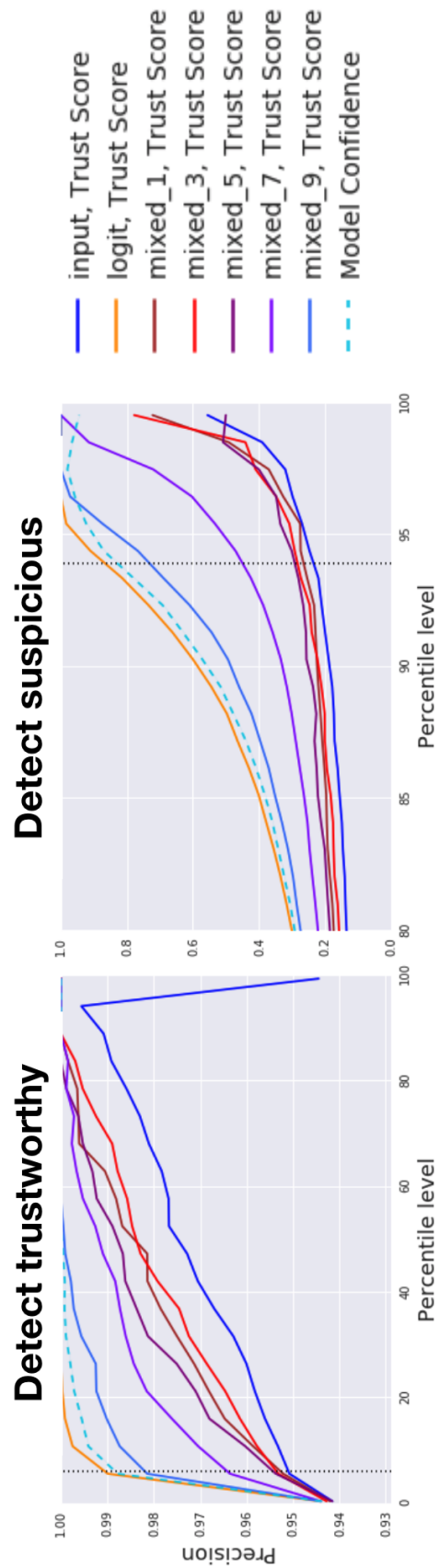


Figure 11: Inception V3: precision on correct (left) and incorrect (right) precision. Higher layers generally seems to achieve better precision.